



Public Inquiry Into Foreign Interference in Federal
Electoral Processes and Democratic Institutions

Enquête publique sur l'ingérence étrangère dans les
processus électoraux et les institutions démocratiques
fédéraux

Public Hearing

Audience publique

**Commissioner / Commissaire
The Honourable / L'honorable
Marie-Josée Hogue**

VOLUME 38

Held at :

Library and Archives Canada
Bambrick Room
395 Wellington Street
Ottawa, Ontario
K1A 0N4

Wednesday, October 23, 2024

Tenue à:

Bibliothèque et Archives Canada
Salle Bambrick
395, rue Wellington
Ottawa, Ontario
K1A 0N4

Le mercredi 23 octobre 2024

INTERNATIONAL REPORTING INC.

<https://www.transcription.tc/>

(800)899-0006

II Appearances / Comparutions

Commission Lead Counsel / Procureure en chef de la commission	Shantona Chaudhury
Commission Counsel / Avocat(e)s de la commission	Gordon Cameron Erin Dann Matthew Ferguson Hubert Forget Leila Ghahhary Benjamin Herrera Howard Krongold Hannah Lazare Jean-Philippe MacKay Kate McGrann Emily McBain-Ashfield Hamza Mohamadhossen Lynda Morgan Siobhan Morris Annie-Claude Poirier Gabriel Poliquin Natalia Rodriguez Guillaume Rondeau Nicolas Saint-Amour Daniel Sheppard Maia Tsurumi
Commission Research Council / Conseil de la recherche de la commission	Geneviève Cartier Nomi Claire Lazar Lori Turnbull Leah West
Commission Senior Policy Advisors / Conseillers principaux en politiques de la commission	Paul Cavalluzzo Danielle Côté

III

Appearances / Comparutions

Commission Staff / Personnel de la commission	Annie Desgagné Casper Donovan Hélène Laurendeau Michael Tansey
Ukrainian Canadian Congress	Donald Bayne Jon Doody
Government of Canada	Gregory Tzemenakis Barney Brucker
Office of the Commissioner of Canada Elections	Christina Maheux Luc Boucher Sébastien Lafrance Nancy Miles Sujit Nirman
Human Rights Coalition	David Matas Sarah Teich
Russian Canadian Democratic Alliance	Mark Power Guillaume Sirois
Michael Chan	John Chapman Andy Chan
Han Dong	Mark Polley Emily Young Jeffrey Wang
Michael Chong	Gib van Ert Fraser Harland

IV Appearances / Comparutions

Jenny Kwan

Sujit Choudhry

Mani Kakkar

Churchill Society

Malliha Wilson

The Pillar Society

Daniel Stanton

Democracy Watch

Wade Poziomka

Nick Papageorge

Canada's NDP

Lucy Watson

Conservative Party of Canada

Nando De Luca

Chinese Canadian Concern Group on
The Chinese Communist Party's
Human Rights Violations

Neil Chantler

David Wheaton

Erin O'Toole

Thomas W. Jarmyn

Preston Lim

Senator Yuen Pau Woo

Yuen Pau Woo

Sikh Coalition

Balpreet Singh

Prabjot Singh

Bloc Québécois

Mathieu Desquilbet

Iranian Canadian Congress

Dimitri Lascaris

V Table of Content / Table des matières

	PAGE
ROUNDTABLE : CANADA’S NATIONAL SECURITY APPARATUS / TABLE RONDE: L’APPAREIL DE SÉCURITÉ NATIONALE DU CANADA	1
Panel moderated by/Panel animé par Dr. Leah West	1
Presentation by/Présentation par Mr. Richard Fadden	4
Presentation by/Présentation par M. Daniel Jean	11
Presentation by/Présentation par Ms. Lex Gill	23
Presentation by/Présentation par Mr. Alan Jones	34
Presentation by/Présentation par Dr. Stephanie Carvin	48
Presentation by/Présentation par Dr. Maria Robson-Morrow	60
Open discussion/Discussion ouverte	70
 ROUNDTABLE : ENFORCING, DETERRING AND PROSECUTING FOREIGN INTERFERENCE ACTIVITIES / TABLE RONDE: MISE EN OEUVRE, DISSUASSION ET POURUITE DES ACTIVITÉS D’INGÉRENCE ÉTRANGÈRE	 113
Panel moderated by/Panel animé par Dr. Leah West	113
Presentation by/Présentation par Dr. Alex Wilner	115
Presentation by/Présentation par Mr. Bob Paulson	122
Presentation by/Présentation par Mr. Croft Michaelson	128
Presentation by/Présentation par Dr. Michael Nesbitt	134
Presentation by/Présentation par Mr. Rob Currie	142
Open discussion/Discussion ouverte	150

Ottawa, Ontario

--- L'audience débute le mercredi 23 octobre 2024 à 9 h 01

--- The hearing begins Wednesday, October 23, 2024 at 9:01 a.m.

COMMISSIONER HOGUE: Bonjour tout le monde.
Good morning. Welcome, and thank you.

I will have the opportunity to thank you at the end, but...

Today the roundtable is entitled a very simple title, actually, today, « L'Appareil de sécurité nationale du Canada », "Canada's National Security Apparatus". And we are lucky enough for having six guests this morning that are well -- widely recognized, actually, as experts in this field for various reasons. Some are coming from the academic world, and others are coming from the field. And the table will be moderated by Leah West, and she will introduce more deeply the various participants -- panellists, I should say.

**--- ROUNDTABLE : CANADA'S NATIONAL SECURITY APPARATUS / TABLE
RONDE: L'APPAREIL DE SÉCURITÉ NATIONALE DU CANADA:**

--- PANEL MODERATED BY/PANEL ANIMÉ PAR DR. LEAH WEST:

DR. LEAH WEST: Sure.

La Commission est chargée d'examiner et d'évaluer la capacité du gouvernement fédéral, y compris de ses agences de renseignement, à détecter, prévenir et contrer l'ingérence étrangère dans les processus démocratiques du Canada.

Le rapport initial de la Commissaire fait

1 état des difficultés rencontrées dans l'identification, la
2 confirmation et l'attribution de l'ingérence étrangère. En
3 particulier, les activités en ligne et dans les processus de
4 prise de décision fondés sur les renseignements et réponses à
5 cette menace.

6 Le rapport aborde également la question de la
7 communication efficace des renseignements et des informations
8 sur les gens... les... l'ingérence étrangère et aux parties
9 prenantes, au public, et aux personnes susceptibles d'être
10 les plus vulnérables à l'ingérence étrangère. Cet aspect du
11 mandat de la Commission peut soulever plusieurs questions.

12 Notamment :

13 "Do Canada's intelligence agencies
14 have the legal authorities, technical
15 capabilities and resources necessary
16 to detect, deter and counter foreign
17 interference? What measures can be
18 taken to make the relationship
19 between Canada's intelligence
20 agencies and government decision-
21 makers stronger? What measures can
22 be taken to improve communications of
23 intelligence and the understanding of
24 the implication of foreign
25 interference threats with external
26 stakeholders, including diaspora
27 communities? What is the current
28 public perception of Canada's

1 national security agencies and, if
2 there is a lack of trust, how has
3 that affected their ability to deter,
4 detect and counter foreign
5 interference, and how should that
6 trust be rebuilt? And should
7 Canada's national security agencies
8 better communicate with the public
9 about the threat of foreign
10 interference and how to protect
11 themselves against it?")

12 So I'm very pleased to introduce our six
13 panellists today. I'm going to introduce them in the order
14 that they will be giving their opening remarks.

15 So we'll be starting with Mr. Richard Fadden,
16 former National Security Advisor and Deputy Clerk, and former
17 Director of the Canadian Security Intelligence Service.

18 Mr. Daniel Jean, former National Security and
19 Intelligence Advisor to the Prime Minister, and former Deputy
20 Minister of Global Affairs Canada.

21 Ms. Lex Gill, a senior Fellow at the Citizen
22 Lab at the University of Toronto.

23 Mr. Alan Jones, former Assistant Director of
24 the -- of Canadian Security Intelligence Service.

25 Professor Stephanie Carvin, Associate
26 Professor at Carlton University.

27 And Dr. Maria Robson-Morrow, who's the
28 program manager at the Harvard Intelligence Project.

1 Each panellist will address these questions
2 in an opening statement and, should time permit before the
3 break, I'll invite a round of responses.

4 So having said that, we'll turn the floor
5 over to Mr. Fadden.

6 **--- PRESENTATION BY/PRÉSENTATION PAR MR. RICHARD FADDEN:**

7 **MR. RICHARD FADDEN:** I would like to start
8 with a couple of what I consider to be meta statements, so
9 they don't directly address the structure issues that Leah
10 has mentioned.

11 I would argue that, generally speaking,
12 outside of the Ottawa bubble, a few academics and a few
13 journalists, the clear and present danger presented by
14 foreign intelligence to our democratic processes is not
15 acknowledged, and I think to the extent that it is not
16 acknowledged and that politicians pay attention to what
17 people think outside of the bubble, I would suggest that it
18 will help the implementation of your recommendations if, on
19 the basis of what you've read and heard, you can say in your
20 report there is a clear, present and serious danger. This
21 has been repeated any number of times, but if you look at
22 polling, generally speaking, it's not accepted that it is a
23 clear and present danger.

24 I think for the countering activities to
25 succeed, the country at large has to be more aware than they
26 are now, I would submit.

27 Second point, I think it will be important as
28 you formulate your recommendations to recognize -- I refer to

1 your FI efforts as within your mandate -- that your FI
2 recommendations will be situated by government within the
3 broader era of foreign intelligence, with foreign
4 interference, which is really quite broad. So expecting the
5 government to go off and set up a whole set of separate
6 institutions, separate legislation and ignoring the rest of
7 FI I think will present governments with challenges and
8 possibly with reasons for not proceeding. So integrating the
9 two, I think, to the extent practical, will be very
10 important.

11 I think that our adversaries who try and
12 engage in foreign interference are sophisticated, they're
13 persistent and they're very well resourced. The only way
14 that we are going to successfully counter them is if we have
15 a whole-of-government and, indeed, a whole of society
16 perspective. And I would argue, I may be a bit at odds with
17 some of my colleagues here, that there is too much of an
18 emphasis on the intelligence or national security community.

19 There is clearly a role for national security
20 and intelligence, but I would say that dealing with foreign
21 interference has to take place on a range of activities: at
22 one end, the RCMP and the courts prosecuting people and
23 sending them to jail if need be, at the other end, some
24 institution or other trying to deal with public education and
25 trying to relieve people's concerns about what is happening,
26 and a whole range of other things in the middle.

27 My point being that I know this is about
28 national security, but I worry a little bit that there's too

1 much emphasis on national security. We have to involve other
2 components of both government and civil society.

3 I think recognizing -- if you accept what
4 I've just said, foreign interference is an ongoing and
5 permanent thing. It is not limited to electoral periods,
6 it's not limited to writ periods, it's ongoing, all the time.
7 And I think if we don't take that point, we're going to miss
8 something very seriously.

9 So slowly coming to the issue of
10 institutions, the role of political parties is obviously
11 very, very important, and we have to find a way of involving
12 them and countering activities without negatively affecting
13 their role in our democratic process, but I think key to this
14 will be keeping Ministers and the Public Service out of this
15 effort to the extent possible.

16 I think it is unreasonable to expect partisan
17 Ministers and partisan players to all of a sudden push a
18 button when they're dealing with foreign interference in
19 these matters and expect them to be entirely non-partisan.
20 And I'll come back to this when I talk about a panel, but I
21 think it's unreasonable to ask public servants who spend
22 their entire lives trying to stay out of partisan politics
23 to, all of a sudden, be the ones who determine what may or
24 may not be done.

25 So political parties, I think, have to be
26 brought between the ambit of regulation or law, but we should
27 set them up as self-regulating and have the panel that I will
28 talk about in a minute be the overseer of this activity.

1 I also would argue that the definition of a
2 political Party may be one that requires a little bit of
3 review. The Liberal Party of Canada, for example, has almost
4 become a movement. You don't have to register, you don't
5 have to pay a fee. I'm not judging whether this is good or
6 bad, but I'm not sure it's going to be easy to have
7 countering activities against movements as opposed to
8 relatively structured political parties.

9 So this gives rise to the question, I think,
10 of what organization can take an interest in overseeing
11 countering activities on a permanent basis.

12 As I said, I think Ministers and Public
13 Service should be kept out of this, so I think the panel as
14 it's presently constituted should be abolished. I would
15 argue that, as I've just said, it's unfair to ask public
16 servants to do that.

17 The Brits have an expression, "the great and
18 the good", and this means, basically, people who have been in
19 public life who've retired and aren't as partisan. I suspect
20 that, with a bit of effort, the government could find a few
21 of these even in Canada, and I would put them on this panel.
22 You know, a former Minister who's, you know, become a
23 statesman, a public servant who's been around for a long
24 time, an academic who has an interest in these matters.

25 I would constitute a panel made up of these
26 people, give them a small secretariat, and make them
27 permanent. I think anything less than permanent oversight of
28 the subject matter is not going to work.

1 I think its operational arm should be a
2 reconstituted Chief Electoral Officer, who should have his
3 writ or her writ extended to political parties, but there
4 should be a relationship between the panel and the Chief
5 Electoral Officer in order to get things done.

6 But I think the particularly important part
7 on this is that the panel should access and have the right to
8 know anything that the intelligence community or the police
9 or anybody else collects on this subject, and they should be
10 able to dialogue and deal with the Chief Electoral Officer on
11 this basis. It has the advantage, I think, of providing
12 permanency and keeping Ministers and public servants out of
13 this issue.

14 One of the issues that we've been asked to
15 look at is whether or not currently the law is sufficient to
16 provide the intelligence communities and others to deal with
17 these issues. I'm not sure I can answer that question
18 absolutely, but I'm a firm believer in making use of the
19 authorities you have before creating new authorities, and I
20 don't think we're doing this across the board.

21 C-70 has barely been registered by the
22 institutions. They're still thinking about how to do it.

23 CSIS has a lot of powers that its risk
24 aversion doesn't allow it to use all the time. I think
25 that's also true of the Mounties. So I would argue that it
26 would be helpful if your recommendations included strong
27 injunction to institutions that currently have authority, use
28 it. Don't be so risk averse, but use it in conjunction with

1 the panel of these great and goods that I'm recommending that
2 you consider.

3 The one element where I do think there is the
4 beginnings of a consensus, I don't think all of these
5 institutions have enough resources. Virtually every other
6 year, there's a new mandate being given to the intelligence
7 communities, and this is a significant one. They still have
8 to worry about traditional espionage, other forms of FI,
9 terrorism and a bunch of other things, and I think it would
10 be unreasonable to expect them to treat this seriously.

11 I think, as I was alluding earlier -- I would
12 argue there's no such thing as national security because
13 there's always a subnational and an international component,
14 and in this respect, I think if we're going to counter your
15 FI efforts, we have to involve the provinces, we have to
16 involve civil society or it's not going to work.

17 The federal government is the most distant
18 level of government from the people in this country, and they
19 find it very difficult to deal on an ongoing basis. Some
20 institutions do better than others, but it was, I think, very
21 similar to how we tried to deal with terrorism.

22 The federal government did a bunch of things
23 at one level, but civil society was best placed to try and
24 deal with people who were thinking about it who are on the
25 verge of doing something negative. So finding a way to have
26 the panel and the Chief Electoral Officer and any other
27 department engage, liaise and actively collaborate with the
28 provinces and civil society I think it's a *sine qua non* to

1 success in this area.

2 The federal government alone, I would submit
3 strongly, cannot counter FI successfully. They just cannot
4 do it. I think this has been proven to be the case in a
5 number of other countries that have also tried to do these
6 things.

7 Just coming back to my panel for a moment, I
8 forgot, I think it should be enshrined in law, but it would
9 be also good if we could do this within our lifetime. So
10 asking the Government of Canada to use existing executive
11 authorities to put it into place, the *Public Inquiries Act* is
12 one way of doing it. If they actually galvanize themselves,
13 it seems to me it would be possible to have such a panel in
14 place before the next federal election, assuming it doesn't
15 happen until May or June.

16 I'm not optimistic, but if we're serious
17 about this, you know, we should get on with it and do
18 something as soon as we possibly can.

19 Lastly, and this is another meta point,
20 having been the recipient on behalf of governments throughout
21 my career of Royal Commission and inquiries' recommendations,
22 I would strongly urge you to prioritize your recommendations.
23 The one thing that governments will do, any Party, is pick
24 and choose the ones that are the easiest or the one that
25 present the most advantage to themselves, so if you
26 prioritize and give them short-, medium- and long-term
27 timeframes in which to be implemented, I think it will be --
28 you will make it easier for government to implement and to

1 avoid going out.

2 I think I'll stop there, and I look forward
3 to any questions that you might have.

4 **COMMISSIONER HOGUE:** Thank you.

5 **MR. RICHARD FADDEN:** Thank you.

6 **DR. LEAH WEST:** Monsieur Jean.

7 **--- PRESENTATION BY/PRÉSENTATION PAR M. DANIEL JEAN:**

8 **M. DANIEL JEAN:** Merci. Bonjour, Madame la
9 Commissaire. Merci de l'invitation.

10 **COMMISSAIRE HOGUE:** Bonjour.

11 **M. DANIEL JEAN:** La Phase 1 de la Commission
12 a fait un travail... un très bon travail, je pense,
13 rétrospectif pour regarder ce qui c'était passé, mais je
14 pense que vous êtes dans la phase la plus critique, celle qui
15 va nous guider en termes d'améliorer la prévention et la
16 dissuasion de l'ingérence étrangère.

17 Bien entendu, le bon fonctionnement de
18 l'appareil de sécurité, c'est un élément clé là-dedans, et
19 c'est ça qu'on va discuter aujourd'hui.

20 Avant qu'on fasse ça, je vais faire deux
21 messages clés. Et, en fait, beaucoup des points d'allocution
22 qui vont appuyer ou vont emmener des nuances sur les choses
23 que monsieur Fadden a dit. Mais deux points qui pour moi
24 sont importants : le premier, le fait que je vais parler
25 d'améliorations qui doivent être faites à la communauté de
26 sécurité et renseignement, ça veut pas dire que j'admire
27 absolument le professionnalisme et dévouement de ces gens-là,
28 alors, de dire qu'on veut des améliorations...

1 **MS. LEILA GHAAHARY:** Excuse me. Mr. Jean,
2 please, could you slow down for the interpreters?

3 Thank you.

4 **M. DANIEL JEAN:** OK. Je pensais que j'étais
5 lent, mais...

6 **(LAUGHTER/RIRES)**

7 **M. DANIEL JEAN:** OK. Alors, d'un premier
8 pas, donc, vraiment, j'admire leur dévouement, et ça veut
9 juste dire qu'on veut améliorer le système. La même chose,
10 un peu comme monsieur Fadden, je vais que ça prend « deux
11 pour tango ». C'est-à-dire que la classe politique doit être
12 engagée. Ils sont très occupés, mais ils doivent être
13 engagés dans ces enjeux-là. Et le fait que je dise ça ne
14 veut pas dire que je ne respecte pas le fait, comment ils
15 sont occupés, et comment le fait que les gens ont le courage
16 de briefer les libertés de suffrage et de servir les
17 Canadiens de nos jours, ça prend du courage.

18 Contexte, je veux pas répéter tous les points
19 que j'ai faits lundi, et puis, Dick vient d'en répéter
20 plusieurs, alors, je veux juste dire, pour moi, les trois
21 plus importants. Les fuites d'information de votre enquête
22 jusqu'à maintenant ont démontré que, en fait, des ingérences
23 peuvent se faire bien avant l'élection. Je dirais que le
24 point le plus important que vous avez fait, le processus de
25 nomination en particulier. Le point que Dick a fait
26 également que les démocraties, c'est beaucoup plus large que
27 juste la question des élections. Et puis enfin, je le
28 rappelle, parce que c'est très important, au moment où on se

1 parle, on a trois procédures criminelles en cours et ils ont
2 lieu avec l'intimidation de la diaspora. Alors, impliquant
3 des pays comme Rwanda, l'Inde et la Chine, mais on sait qu'il
4 y a d'autres pays qui sont impliqués dans ces choses-là.

5 Moi, j'ai essayé à la fois des questions qui
6 ont été posées, mais également regarder les enjeux qui ont
7 été levés jusqu'à maintenant dans la Commission pour
8 identifier ceux qui m'interpellent par rapport à l'appareil
9 de sécurité nationale.

10 Alors, j'en ai identifié six. Le premier
11 qu'on a parlé, le manque de culture de sécurité nationale, ce
12 qui veut dire que on ne met pas d'attention sur les
13 évaluations les plus stratégiques et qu'on a tendance à
14 toujours faire la mise à jour de nos instruments juridiques
15 en temps de crise.

16 Mon deuxième point, défi de développer des
17 produits de renseignement de qualité et avec les différents
18 degrés de fiabilité clairement énoncés. On a eu un petit peu
19 un échange là-dessus lundi, Madame la Commissaire. Je vais y
20 revenir avec un petit peu plus de matière.

21 Troisièmement, la dissémination de ces
22 produits-là auprès des fonctionnaires clés, mais également
23 les responsables politiques pertinents pour guider leurs
24 actions, si nécessaire et possible.

25 Quatrièmement, l'approche un petit peu plus
26 systémique de s'assurer que les menaces les plus sérieuses
27 sont amenées à l'attention des gens importants, que ce soit
28 au gouvernement, dans les partis politiques, ou autre. Et

1 que il y ait un système vraiment en place pour acquiescer et
2 documenter la prise de connaissances de ces choses-là.

3 Cinquièmement, on vit dans un monde où les
4 joyaux de la Couronne sont de plus en plus à l'extérieur du
5 gouvernement. Alors, la nécessité pour les agences de
6 sécurité d'opérer un changement culturel fondamental pour
7 mieux alerter et soutenir les Canadiens contre les différents
8 types d'étrangère.

9 Et sixièmement, j'ai parlé un petit peu de
10 la... l'importance d'avoir une bonne gouvernance horizontale,
11 tant chez les fonctionnaires qu'au Cabinet, pour être capable
12 de vraiment porter l'attention sur ces enjeux-là.

13 Je passe par le premier. Le premier, je peux
14 passer assez rapidement. J'en ai parlé lundi. J'abonde
15 beaucoup dans ce que Dick a dit. On n'a pas de culture de
16 sécurité nationale. Si les Canadiens s'intéressent pas à ça,
17 les politiciens s'intéresseront pas à ça. Et,
18 malheureusement, ça veut dire que les Canadiens s'intéressent
19 à ça en... dans le milieu de crise, et les politiciens
20 s'intéressent à ça en milieu de crise, et ça fait qu'on a
21 tendance à toujours faire nos lois en temps de crise. La *Loi*
22 *sur le SCRS* a été créée après le scandale à la GRC en 84. La
23 *Loi de 2015* était une réaction aux évènements terroristes.
24 Et puis on a la loi C-70 en un temps record, parce que,
25 encore une fois, on a une crise dans l'ingérence étrangère.

26 Il y a un effort, à travers la création d'un
27 Conseil de sécurité nationale comme comité de Cabinet,
28 d'essayer de changer ça, de regarder, d'avoir des

1 discussions. C'est très tôt, alors, c'est très tôt pour
2 porter le jugement.

3 Parlons maintenant du deuxième défi, celui de
4 développer des produits de renseignement de qualité avec des
5 degrés de fiabilité clairement énoncés. Les délibérations de
6 votre comité, pis en particulier quand on voit la lecture que
7 les gens ont fait pis les interprétations différentes qu'ils
8 ont fait, en particulier du matériel qui soutenait le rapport
9 du Comité des parlementaires sur la sécurité nationale et le
10 renseignement, nous montre comment des gens peuvent lire tous
11 les mêmes documents et arriver à des interprétations
12 différentes.

13 Pour moi, pis c'est mon expérience dans la
14 bureaucratie, ça me dit que peut-être que nos gens qui
15 écrivent ces rapports-là ont tendance à écrire pour eux-mêmes
16 plutôt que pour des auditoires qui ne sont pas des experts.
17 C'est pas un problème juste dans la sécurité nationale, je
18 peux vous en parler pendant 35 ans.

19 Alors, il faut vraiment revoir ça. Et là-
20 dedans, il y a la question que vous avez soulevée qui était
21 déjà dans mes remarques que j'avais écrit pour aujourd'hui -
22 très bon point, Madame - ça peut pas se faire dans un vide.
23 Le renseignement est indépendant, la collecte, l'analyse,
24 mais il peut pas se faire dans un vide. Il faut qu'il y ait
25 un échange avec les auditoires. Le renseignement, il est
26 neutre au niveau des politiques et des opérations. Eux, ils
27 doivent respecter l'indépendance, mais ils vont gagner : la
28 valeur ajoutée va être là, les produits vont être meilleurs

1 et on va être beaucoup mieux servi par tout ça.

2 Alors, si... je le dirais, puis je l'ai décrit
3 tout à l'heure, il y a eu énormément de progrès dans
4 l'habilité de la communauté de la sécurité nationale à
5 travailler horizontalement entre eux. Je dirais qu'au niveau
6 du renseignement, c'est un des points où on doit faire le
7 plus d'améliorations.

8 Troisième point, la dissémination de ces
9 produits auprès des fonctionnaires clés et des responsables
10 politiques pertinents qui puissent guider les actions, si
11 nécessaire et possible. Comme de raison, si nécessaire et
12 possible, 95 pour cent et plus des rapports de renseignement
13 que l'on lit, soit n'invitent aucune action ou, si jamais il
14 pourrait y avoir une action, souvent, c'est les agences qui
15 voulaient pas qu'on le fasse parce qu'on doit protéger les
16 méthodes, les sources et des enquêtes qui peuvent être en
17 cours. Donc, c'est pour ça que je dis si nécessaire et si
18 possible.

19 Quand je dis qu'on doit apporter ces
20 documents-là, disséminer aux différents auditoires, il faut
21 aller plus loin que les auditoires traditionnels. Bien
22 entendu, le Comité de sécurité et renseignement doit
23 constamment travailler avec les ministères dans la
24 communauté, mais également avec les ministères économiques.

25 Vous avez une très belle étude de cas dont la
26 Commission pourrait s'inspirer sur comment la réponse du
27 Canada à la sécurité économique à partir de 2016, comment des
28 ministères qui se parlaient pas, Innovation, sciences et

1 technologies ont travaillé avec la communauté de sécurité
2 nationale. Vous avez juste à regarder les statistiques sur
3 la *Loi sur Investissement Canada*, vous allez vous apercevoir
4 que vous avez une très, très belle étude de cas où le système
5 a fonctionné. Pourquoi que ça a fonctionné? Parce que les
6 fonctionnaires ont bien travaillé ensemble, ils ont réussi à
7 engager le Cabinet et le Cabinet a fonctionné.

8 Lettre de mandat du ministre disait qu'il
9 devait amé... accroître l'investissement étranger à une époque
10 où beaucoup de ces investissements étrangers-là venaient de
11 la Chine et étaient préoccupants. Le système a fonctionné
12 parfaitement. Ça me ferait plaisir de vous remettre un
13 paragraphe là-dedans dans le rapport qu'on devra mettre.

14 Il faut maintenant, c'est un point qui est
15 important, beaucoup de rapports. La classe politique, ils
16 sont occupés, les ministres sont occupés, le Premier ministre
17 est occupé, ils peuvent pas lire, ils peuvent pas savoir
18 tout. Il faut choisir qu'est-ce qu'ils ont vraiment besoin
19 de voir. Il faut également avoir même chose pour les partis
20 politiques, les joueurs importants, les parlementaires.

21 Maintenant, il faut trouver une façon de..
22 capable de mettre un petit peu plus d'imputabilité dans le
23 système pour tout le monde. Il faudrait qu'on sache décrire
24 qu'est-ce qui a été breffé, que le contenu soit connu, pas
25 nécessairement publiquement, le contenu est connu, pis c'est
26 documenté.

27 Mon cinquième point, on vit dans un monde où
28 les bijoux de la Couronne sont de plus en plus à l'extérieur

1 du gouvernement. Et je sais que Maria va parler beaucoup de
2 ça. C'est la nécessité pour les agences de sécurité d'opérer
3 un changement culturel fondamental. Qu'est-ce que je veux
4 dire par « les joyaux de la Couronne sont de plus en plus à
5 l'extérieur du gouvernement »?

6 Les technologies sensibles dans le secteur
7 privé et les secteurs de recherche dans les universités et
8 instituts; la manipulation via une désinformation systémique
9 pouvant diviser et affaiblir la confiance dans les
10 institutions démocratiques; le suivi, le harcèlement et
11 l'intimidation des diasporas dans le but de faire taire des
12 critiques ou dissidences; le rôle fondamental des partis
13 politiques dans notre démocratie, d'où l'effort d'essayer de
14 les influencer; le fait que certains de ces joyaux de la
15 Couronne et vulnérabilités se retrouvent dans divers paliers
16 de gouvernement : provinces, territoires, municipalités et
17 gouvernance.

18 Il y a des efforts qui ont été commencés sous
19 Michael Warnick et qui ont continué avec les autres greffiers
20 où on fait des échanges avec les provinces et territoires,
21 mais il faut que ça devienne plus systémique et dans les
22 niveaux inférieurs.

23 Maintenant, ils doivent également pouvoir
24 étudier à bon escient les autorités existantes, les nouvelles
25 autorités par exemple que C-70 va donner à la... au SCRS pour
26 partager davantage la nature de la menace et sa manifestation
27 tout en protégeant les sources, les méthodes et les enquêtes.
28 Ça demande un changement culturel profond. Et un changement

1 culturel profond, la façon dont on fait ça, c'est dans la
2 façon dont on recrute, qu'on forme et qu'on encourage avec
3 les bonnes incitatives ce qu'on veut de ce côté-là.

4 Et je suis tout à fait d'accord avec Dick
5 également que d'amener une lentille sécurité nationale n'est
6 pas juste la responsabilité de la communauté de la sécurité
7 nationale, les gens dans les autres ministères doivent le
8 faire, et c'est un peu ce qu'on a réussi à faire au niveau de
9 la sécurité économique.

10 Alors, qu'est-ce que ça peut vouloir dire,
11 mettons, pour quelques-uns des joueurs? Pensons au CST.
12 C'est intéressant, le CST était l'Agence du gouvernement la
13 plus secrète, mais la menace de la cybersécurité les a
14 forcés, à travers la création du Centre de sécurité sur la
15 cybersécurité, à avoir vraiment un dialogue avec les
16 populations sur la menace cyber.

17 Le virage est entamé au CST, mais je dirais
18 qu'il a été entamé dans le continuum à ce qu'on appellerait
19 la connaissance, alerter d'un point de vue information. On
20 doit aller beaucoup plus loin sur la résilience. Si on avait
21 un JBS Foods où 30 pour cent du bœuf pis du porc est
22 paralysé, si on avait un Colonial Pipeline où une bonne
23 partie de l'approvisionnement en énergie est paralysé par une
24 attaque cyber, est-ce qu'on est prêt pour ça?

25 Pour le SCRS, le virage requis est
26 considérable parce que, jusqu'à maintenant, ils ont été
27 beaucoup menottés. Ce qu'ils auraient dû être capables de
28 faire à l'extérieur, leurs lois leur permettaient pas et ils

1 allaient le plus loin souvent qu'ils pouvaient. Mais il y a
2 également parce que leur culture interne est vraiment de
3 jouer le *inside baseball*. Et ça, ça a demandé un virage
4 culturel vraiment, vraiment important.

5 Maintenant, en ce qui concerne la GRC, pis je
6 donnerai pas de recommandation sur ce que devrait être la
7 structure, mais il faut résoudre le conflit quant à la
8 capacité de la GRC de jouer pleinement son rôle de police
9 fédérale, quand la majeure partie de son attention et les
10 ressources, 70 pour cent, c'est la police contractuelle. Il
11 faut avoir le courage de trouver une solution à ça.

12 Mon dernier point, peut-être le plus
13 important compte tenu du panel, la gouvernance horizontale.
14 Tout d'abord, au niveau des fonctionnaires, il y a eu des
15 progrès énormes depuis la création du rôle de conseiller de
16 la sécurité nationale, comme on le connaît, qui est en 2003.
17 En particulier, l'agilité à répondre de manière cohérente et
18 coordonnée aux crises, très, très bien.

19 J'ai dit tout à l'heure qu'on doit faire des
20 améliorations dans comment le renseignement est fait et qu'il
21 devrait pas se faire dans un vide. Au niveau des
22 développements des politiques, ça... c'est pas parfait, mais
23 ça... il y a quand même de bons efforts qui sont faits pour une
24 horizontalité dans le développement des politiques qui sont
25 le mandat du gouvernement. Puis également, d'avoir un œil
26 sur ce qui s'en vient. D'avoir un œil sur ce qui s'en vient,
27 c'est ça qui a permis au Canada et aux États-Unis d'être les
28 deux pays qui ont probablement bougé le plus vite sur les

1 enjeux de sécurité économique.

2 Maintenant, je l'ai dit tout à l'heure, il y
3 a jamais vraiment eu d'espace, de temps, les gouvernements
4 antérieurs, tous partis confondus, ont essayé un moment donné
5 de créer des comités de cabinet pour des discussions
6 stratégiques. Ça ne s'est pas passé. On a maintenant un
7 conseil de sécurité stratégique. J'espère que ça va nous
8 donner cet espace-là, mais il est juste trop tôt pour rendre
9 conclusion.

10 Maintenant, parlons du rôle du conseiller de
11 la sécurité nationale, qui est une clé dans cette gouvernance
12 horizontale-là, tant au niveau des fonctionnaires mais de son
13 lien avec le Premier ministre pis le Cabinet.

14 Comme je l'ai dit lundi, moi, j'ai aucune
15 objection à cette suggestion de codifier le rôle du
16 conseiller à la sécurité nationale dans la loi, mais je pense
17 qu'on a des attentes qui sont peut-être... sur l'impact que ça
18 aurait qui sont peut-être un peu exagérées. Parce que à
19 moins qu'on va remettre en question le modèle de Westminster,
20 où les responsabilités demeurent sous les ministres et leurs
21 institutions, cette codification, elle va juste venir
22 confirmer le rôle de la fonction.

23 Et, à mon avis, le rôle de la fonction, c'est
24 le miroir du Conseil privé, pis c'est trois rôles
25 fondamentaux. Le premier c'est un avis indépendant au
26 Premier ministre. Le deuxième, c'est le support et avis au
27 Cabinet. Le conseiller de la sécurité nationale, un peu
28 comme le greffier du Conseil privé, travaille de très, très

1 près... le travail, par exemple, pour amener la sécurité
2 nationale, la loi fiscale de 2019, que j'ai fait avec le
3 ministre Goodale à l'époque, son sous-ministre Malcolm Brown,
4 c'est des facteurs fondamentaux pour pouvoir avancer
5 rapidement des législations. Et c'est une législation qui a
6 été très, très bien reçue dans le public.

7 Il y a beaucoup de similarités entre les
8 attributs requis pour être un bon conseiller à la sécurité
9 nationale pis un bon sous-ministre de portefeuille. Dick va
10 comprendre ce que je veux dire par là. Parce que les sous-
11 ministres de portefeuille également, si vous êtes à
12 Transport, si vous êtes à Innovation, si vous êtes à
13 Patrimoine, il y a une multitude d'acteurs indépendants. Ils
14 se rapportent pas à vous, mais vous devez donner des avis
15 indépendants au ministre sur comment ils pourraient mieux
16 faire. Puis il veut également amener une certaine cohérence
17 et coordination entre eux.

18 Je vais faire une révélation qui ne sera pas
19 une révélation pour Dick. Certains de nos meilleurs sous-
20 ministres sont extrêmement inconfortables dans des positions
21 d'être sous-ministre de portefeuille, de la même façon que
22 d'être le conseiller de la sécurité nationale est pas fait
23 pour les mêmes... tous les sous-ministres, même s'ils sont
24 très, très compétents.

25 Pour moi, les attributs du conseiller de la
26 sécurité nationale sont d'être une personne expérimentée et
27 respectée de ces pairs pour pouvoir jouer ce rôle, d'amener
28 cohérence et coordination, et également de mettre au défi les

1 hypothèses ou les propositions. Il y a une *challenge*
2 *function*, comme le rôle de PCO.

3 Deuxième rôle, la capacité d'offrir ce qu'on
4 appelle cette *fearless advice*, les « avis sans crainte » dans
5 le modèle de Westminster, aux auditoires clés du Premier
6 ministre et Cabinet. C'est pas, à mon avis, un accident que
7 plusieurs des conseillers étaient des gens qui sont arrivés à
8 leur dernier poste avant la retraite, parce que ça vous donne
9 cette liberté d'être capable de donner la *fearless advice*.

10 Et mon troisième point qui peut démontrer sa
11 valeur ajoutée tant à la communauté que les auditoires comme
12 le Premier ministre et le Cabinet. Quand on fait
13 l'orientation des sous-ministres, on leur explique toujours
14 qu'être un sous-ministre, c'est être un sandwich entre une
15 institution et un ministre, parce que l'institution pense
16 toujours que vous faites pas assez pour faire comprendre au
17 ministre qu'ils savent c'est quoi les bonnes affaires, et les
18 ministres pensent toujours que vous poussez pas assez
19 l'institution pour ce qu'elle veut faire.

20 Un bon conseiller à la sécurité nationale et
21 au renseignement est quelqu'un qui va être un bon lien entre
22 les deux et non pas l'amplificateur de l'un ou de l'autre.

23 Je vais en arrêter là. J'ai hâte à la
24 discussion. Merci.

25 **COMMISSAIRE HOGUE:** Merci beaucoup.

26 **DR. LEAH WEST:** Merci beaucoup. Maître Gill?

27 **--- PRESENTATION BY/PRÉSENTATION PAR MS. LEX GILL:**

28 **MS. LEX GILL:** Bonjour. Good morning,

1 Commissioner, colleagues. Thank you for having me. While
2 the views that I'm sharing this morning are my own, they're
3 informed primarily by the longstanding work of the Citizen
4 Lab, which is an interdisciplinary organization that conducts
5 both technical and investigative research regarding digital
6 threats to civil society, as well as legal and policy
7 analysis at both the domestic and international level
8 regarding issues at the intersection of information and
9 communications technologies, human rights and global
10 security.

11 I'm also a litigator with a practice broadly
12 focused on constitutional law, human rights and state
13 liability, and a background representing civil liberties
14 groups, and so I'm bringing all of those perspectives to my
15 comments today, which means that, at this table, I'm a little
16 bit of an outsider, and I want to use that perspective to
17 perhaps offer a bit of friction or critical insight for my
18 comments today.

19 And in that spirit, there are essentially
20 three issues I'd like to raise this morning. First, I want
21 to talk about the role of the *Charter* and how we think about
22 new national security powers. Then I want to talk about how
23 -- or I want to talk about some of the constitutional issues
24 that come up when we talk about foreign contact. And
25 finally, I want to share some thoughts on the particular
26 issue of digital transnational repression all through the
27 lens of Citizen Lab's work.

28 So some of the discussion questions for the

1 Commission go to the adequacy of the existing powers and
2 capabilities of Canada's intelligence agencies, and I want to
3 speak to those questions.

4 In response to complex problems like foreign
5 interference, the reflex is often to demand more, more power,
6 more funding, more resources, more information sharing. Our
7 Constitution nonetheless imposes very strict limits on both
8 legislation and government action for good reason including
9 the sphere of national security and intelligence. And in
10 that sphere, we need to exercise particular care and
11 attention with regard to the impacts of these potential new
12 powers on freedom of expression, on privacy, on the rights to
13 liberty and security of the person, on equality rights, the
14 right to non-discrimination. There is simply nowhere else in
15 Canadian law where the state is entitled to act with so much
16 latitude, exercise so much power, access so much information
17 and impact the lives of so many people.

18 And we know that errors and abuses can have
19 very grave consequences on individuals, on their futures, on
20 their families, on their status in Canada, and this is all
21 the more true because in the national security context, the
22 powers engaged are particularly difficult, in some cases
23 almost impossible to meaningfully review. And the ability to
24 engage in a full adversarial process is often necessarily
25 limited by the evidentiary and intelligence constraints at
26 play. And we have to admit too that Canadian intelligence
27 bodies have a less than perfect record before our courts and
28 before the Federal Court, in particular, on these issues.

1 This is not meant to suggest that there are
2 no protections or safeguards in place, and I would say that
3 over the last 10 years there have been significant gains in
4 this regard, especially through the wide reforms adopted in
5 C-59. But the fact remains that this is an area where the
6 stakes are very high, the powers are extensive, review is
7 mitigated at best, and the cost of getting it wrong can be
8 incredibly serious, both for individuals who are affected and
9 for the integrity and legitimacy of our public institutions.

10 You know, over the summer we saw a rush to
11 pass a series of complex legislative reforms under the banner
12 of C-70, despite real and legitimate, I think, concerns from
13 a broad spectrum of civil society groups that there was not
14 adequate consultation or review regarding those powers, and
15 concern that those new rules were complex, that they would
16 have significant implications for human rights and *Charter*
17 rights in Canada.

18 And I would just say that, as a result, no
19 matter how serious the threat, you know, and this is not to
20 call into question the seriousness of the threat or how
21 pressing the government's objective is, I do want to ask the
22 Commission to keep the *Charter* as well as fundamental
23 democratic principles like openness and transparency and the
24 rule of law at the very heart, at the forefront of its
25 analysis. We have to start from that place.

26 And in that spirit, it's obvious, but we have
27 to remember that the Constitution binds the entirety of the
28 state in Canada including Canada's national security bodies.

1 You know, while the Supreme Court's approach to the
2 extraterritorial application of the *Charter* leaves something
3 to be desired still, I think Dr. West, I agree with her work
4 that -- to the extent that there should be a sort of *Charter*
5 unless approach. It's the only coherent way forward, but,
6 you know, apart from that issue, there's really no doubt that
7 the *Charter* does apply to everything, everything Canada's
8 intelligence agencies do in Canada in relation to people in
9 Canada, and in relation to infrastructure in Canada.

10 And so that means that not only do any new
11 powers need to be restrained by our Constitution and the
12 jurisprudence that interprets the scope of *Charter* rights,
13 but also that those powers need to be meaningfully subject to
14 real *Charter* review by the courts, through real adversarial
15 processes, with real remedies available when the state gets
16 it wrong. And there's surely work to do in that regard.

17 So in a similar vein, I want to make things a
18 little bit complicated, I want to make a few comments about
19 the attempt to regulate and control specifically foreign
20 interference and influence from a *Charter* perspective. And
21 this is because in this -- in these conversations, the scope
22 of *Charter* applicability can sort of sit uncomfortably
23 alongside some of the ways that we talk about foreign
24 interference and the role of Canada's intelligence agencies.
25 Of course, we don't think of foreign states as having
26 constitutional rights in Canada. They certainly don't. But
27 when we're talking about foreign interference, we know that
28 states ultimately operate through people, and it is so -- so

1 it's through people in Canada, you know, it's those people in
2 Canada who are subject to suspicion, to surveillance, to
3 intelligence gathering, to investigation, to threat
4 disruption activities, immigration consequences and criminal
5 investigation and sanction. And those people have
6 constitutional rights.

7 So when we talk about the influence -- when
8 we only talk about the influence of foreign states, we sort
9 of abstract away that reality. We tend to talk about the
10 rights engaged by these issues through the lens of
11 citizenship, or through the lens of the interests of
12 Canadians. But for almost all constitutionally protected
13 rights, with only a few exceptions, the *Charter* doesn't apply
14 to Canadians. It applies to everyone, to everyone. So
15 there's no second-class rights framework for non-citizens as
16 far as the *Charter's* protections, for freedom of expression,
17 for privacy, for security of the person, for equality are
18 concerned.

19 And obviously, no one here is arguing that
20 foreign interference is not a serious threat, but that fear
21 can't legitimize a political or legal narrative that would
22 rationalize a discount on the *Charter* protections available
23 to non-citizens in Canada. That's not just a question of
24 principle, it's also because the stakes can be high and
25 because that issue goes really to the legitimacy of our
26 intelligence agencies, the legitimacy required to be able to
27 do effective intelligence work.

28 So finally, I want to summarize some of

1 Citizen Lab's recent research on digital transnational
2 repression in Canada, particularly as detailed in a 2022
3 report that I'll include in my written comments from my
4 colleagues Noura Al-Jizawi, Siena Anstis and others, and I
5 want to invite the Commission to really look seriously at
6 this question in its final report. We all know that
7 authoritarian states don't stop at their borders when
8 attempting to suppress dissent and criticism. We know this
9 from publicly reported cases, as my colleagues mentioned, of
10 foreign states working to silence or coerce nationals working
11 on human rights issues in particular outside of their
12 territorial reach, including Saudi Arabia, Rwanda, China,
13 others. In this way, the Lab's research really builds on
14 that body of work related to transnational repression and
15 explores the ways in which it evolves through digital
16 technologies, and we think this is really, really critical to
17 understanding the next few years.

18 And the team's research demonstrates that
19 digital transnational repression is rapidly becoming the
20 cornerstone of everyday transnational repression, and it's a
21 particular threat to the rights and freedoms of dissidents
22 and activists living in exile. We're really talking here
23 about a constellation of activities, online harassment,
24 intimidation, threats, doxing, surveillance, use of spyware
25 and malware, targeted leaks and hacks, coercion by proxy,
26 including through intimidation of allies, friends, and family
27 back home. And I guess noting importantly that digital
28 technology gives authoritarian states just huge new

1 visibility into those relationships and into the most
2 intimate spheres of people's lives.

3 This kind of activity is both enormously
4 common and it's particularly challenging, because unlike
5 direct human interactions, the digital context is seen as
6 lower cost, as scalable, as harder to detect, and accompanied
7 by lower risks of sanction or accountability for state actors
8 that engage in it, both because attribution is difficult and
9 because these behaviours may be more -- less likely to be
10 seen as an attack on sovereignty.

11 I would add that women in particular face
12 qualitatively and quantitatively different kinds of risks in
13 terms of digital transnational repression, and this is an
14 area of the Lab's future research that I think is
15 tremendously important.

16 In Canada, the research demonstrates this
17 kind of foreign interference has very serious impacts on
18 activists and dissidents in diaspora communities, including
19 on their ability to undertake transnational advocacy work
20 related to human rights, which, of course, goes to Canada's
21 interest abroad as well.

22 In addition to direct threats to safety and
23 security, the result of these activities is a global chilling
24 of political and social speech that disproportionately
25 impacts the freedom of certain groups in Canada, so not just
26 what you're going to say at a local meeting, but also what
27 you're going to say and do online, through communications
28 platforms, and the extent to which you can meaningfully

1 connect with collaborators and loved ones in your home
2 country and that disproportionate impact is serious.

3 The Lab's research concludes that support for
4 victims and the Canadian government's response in this area
5 has been seriously inadequate. It's partly because in Canada
6 the focus on foreign digital threats has overwhelmingly been
7 in relation to formal democratic institutions and economic
8 interest and critical infrastructure, but it's also because
9 these individuals and groups are already vulnerable and
10 marginalized in our society. They're already criminalized.
11 They're already underserved by our legal and political
12 institutions.

13 And so in addition to that marginalization,
14 these are now people who are still subject to the
15 consequences of authoritarianism, even after leaving their
16 country of origin, and are nonetheless taking often very
17 major personal risks to defend human rights and democratic
18 values at a personal cost, and we have to do more for these
19 people.

20 MS. LEILA GHAAHARY: Excuse me, Ms. Gil,
21 could you ---

22 MS. LEX GILL: Yeah.

23 MS. LEILA GHAAHARY: --- please slow down for
24 the interpreter?

25 MS. LEX GILL: No problem.

26 MS. LEILA GHAAHARY: Thank you.

27 MS. LEX GILL: Yeah, thank you. So the Lab's
28 report does detail a series of recommendations. Some of

1 those Canada has made some headway to adopt since the report
2 was published in 2022, including better coordination across
3 government bodies, and greater public communication, and more
4 support for victims. So too though on that list was the need
5 to ensure that the Canadian government's own use of digital
6 surveillance technology was transparent, is transparent,
7 lawful and rights respecting, as well as the need for greater
8 transparency from technology companies regarding how they
9 respond to government requests to remove content or access
10 user information as part of efforts to respond to digital
11 transnational repression.

12 Similarly, the Lab has said Canada needs to
13 do more to sanction companies and needs to refuse to do
14 business with companies involved in developing and selling
15 the technology that facilitates these abuses by authoritarian
16 regimes like spyware manufacturers.

17 And so in this sense, these recommendations
18 bring us back to my first point and perhaps the thing that
19 unites all of my comments this morning, which is really just
20 an observation about trust, legitimacy, respect for the
21 Constitution and the rule of law at home. Our research shows
22 that even, you know, for example, when somebody did choose to
23 reach out to CSIS or law enforcement in a case of digital
24 transnational repression, the result is that they felt it was
25 useless or even harmful, if they got a response at all.

26 As the Commissioner already knows, legitimate
27 concerns about abuse, overreach, discrimination and
28 criminalization all undermine any incentive that someone

1 might otherwise have to collaborate, leaving these
2 communities on their own and leaving us all less safe. And I
3 would just add, in that respect, that while maybe the people
4 at this table or the people in this room can make kind of
5 clear distinctions between different intelligence agencies,
6 or the difference between intelligence and law enforcement,
7 or the difference between intelligence and immigration, that
8 is not the case for ordinary people on the ground. It is the
9 state of Canada and the -- especially now that we're in an
10 environment where there is so much more information sharing,
11 I have to say that that distinction is less and less real
12 even within government. And so I think that we have to be
13 sensitive to the reality that that is the perception from
14 individual people who are affected by these kinds of abuses.

15 So, ultimately, I'm hopeful that the
16 Commission is going to conclude that the legal constraints
17 and democratic values that I'm talking about are worthy for
18 their own sake, and that they need to be a starting point for
19 any analysis, but it's also clear that without them Canada's
20 intelligence agencies and law enforcement authorities and
21 legal institutions are just going to lack the basic
22 legitimacy they need to act effectively.

23 So I think I'll stop there. It's really only
24 through a legal and political culture that's irreproachable
25 in terms of its respect for its constitutional obligations
26 and human rights and civil liberties that Canada's
27 intelligence agencies will be able to make meaningful inroads
28 in addressing these threats. Thanks.

1 DR. LEAH WEST: Thank you very much. I'll
2 turn to Mr. Jones.

3 ---PRESENTATION BY/PRÉSENTATION PAR MR. ALAN JONES:

4 MR. ALAN JONES: Thank you. Good morning,
5 Commissioner. Thank you for the opportunity to speak. My
6 panel of colleagues have covered a lot of ground, some of
7 which I was going to cover, so I've removed some of that, so
8 if I -- it appears a bit choppy, it's because I do not want
9 to do -- repeat some of the things that I agree with from my
10 colleagues.

11 The vast majority of foreign interference
12 campaigns in Canada are not the most egregious criminal acts
13 of some of which we've talked about in this past year with
14 regarding Government of India and the murder of Mr. Nijjar.
15 The majority of foreign interference campaigns are going to
16 be conducted at a more subtle level, some involving
17 intimidation broader, but not hitting that high bar that we
18 have seen and have talked about this year. But there is a
19 trend for adversary states to become increasingly aggressive
20 and use tactics to cross red lines. Murdering people and
21 violating sovereignty is not typical of what foreign
22 interference campaigns have been traditionally, but they seem
23 to be becoming more popular and there seems to be almost with
24 a perceived impunity to be able to do this.

25 This disturbing trend was directly addressed
26 recently by Ken McCallum, who's the Director-General of MI5,
27 the British Security Service, in a public statement the last
28 couple of weeks, where he was referring primarily to the

1 actions of the Russian government, including the murder of
2 dissidents in the United Kingdom, also states such as Iran.

3 Mr. McCallum went so far as to say that
4 Moscow was seeking to cause mayhem on the streets of Europe.
5 It is a continent at war, and that war is touching Canada.
6 Canada is not immune to these types of threats.

7 There's been similar statements made by Mike
8 Burgess, who's the Director-General of the Australian
9 security intelligence organization. Australia created a
10 foreign interference threat assessment centre about three
11 years ago intentionally focused on the issue of foreign
12 interference, somewhat like a terrorism threat assessment
13 centre, but focused on foreign interference. And Mr.
14 Burgess's comment was that the average Australian would be
15 surprised at the depth and the breadth of foreign
16 interference that is occurring in Australia.

17 In the Canadian context -- that may be a
18 reference point to us, but in the Canadian context, I
19 completely agree with previous comments that this needs to be
20 addressed by not just government, but by civil society and by
21 academia. And I can give you an example of that,
22 Commissioner.

23 So when I retired from CSIS, I began working
24 with the University of Ottawa on a national security program
25 because I was of the view that there is a level of illiteracy
26 about the national security issue in Canada, writ large, at
27 every level, including at senior levels of government. I
28 blame no one for this. This is just part of our culture and

1 it's just part of the reality, but also in public as well.

2 There was a lot that we could talk about in
3 public that has not been discussed previously that we need to
4 talk about publicly. It's important to our democracy.

5 So we created a national security program at
6 the University of Ottawa Professional Development Institute.

7 One of -- or a couple of the areas that we
8 have been looking at is gender disinformation focused on
9 women and young girls as well as foreign repressive
10 governments targeting women journalists in the West. Freedom
11 of the press is integral to our democratic process.
12 Protection of women from gender disinformation is integral to
13 our democratic values.

14 Yesterday, the U.S. Department of Justice
15 laid charges against a senior General in the Iranian
16 Revolutionary Guard Corps, along with eight others, for an
17 assassination plot against an Iranian U.S. journalist named
18 Masih Alinejad.

19 Today, as we speak here or talking here, Ms.
20 Alinejad is speaking at the University of Ottawa. We brought
21 her up from the United States, police protection, and she is
22 holding an event where she is explaining personally what her
23 experiences are and what she has received in the form of
24 disinformation and threats from a foreign government in the
25 United States, and the same thing is happening here in
26 Canada.

27 That is the type of thing where you can have
28 government, civil society and academia collectively working

1 to shed light on issues such as this as foreign interference.

2 I'll also add that foreign interference in
3 the federal electoral process and democratic institutions is
4 only a part of foreign states' foreign interference
5 strategies. No state really has a strategy solely to
6 interfere in the election process in Canada. It's part of a
7 much larger process of their foreign policy of projecting
8 power and dealing with dissidents and changing the
9 environment to their advantage.

10 So we're entering a stark era where
11 traditional foreign interference has tended to be meddling
12 and with intimidation, is now including extreme acts of
13 violence and threats of violence. And as with most national
14 security threats, as Dick mentioned, these threats don't
15 replace traditional threats. They simply become yet another
16 layer on top of all the other threats that you have to deal
17 with.

18 Government of Canada's responses will need to
19 be as layered and as nuanced as the threat itself, from
20 subtle to sometimes blunt, i.e. arrests and law enforcement.
21 The law enforcement is going to be, I think, an exceedingly
22 rare occurrence in this space.

23 CSIS, the RCMP, CSE, in my opinion, have lots
24 of investigative powers. They have plenty of powers. But as
25 Dick said, they need to be -- they need to be maximized in
26 how they're used within constitutional law, within
27 constraints, within review.

28 Investigative powers is -- you know, is a

1 direct and somewhat easy way to deal with these issues. It's
2 far more complicated to build the expertise and develop
3 coherent frameworks around the investigation of threats from
4 foreign interference.

5 Coherent strategies require building and
6 maintaining expertise on complex issues such as ethnic,
7 political, irridentist trends amongst diaspora requires
8 specific focus on these issues. The knowledge to understand
9 what foreign interference is in its many forms and looks like
10 comes with experience. It's not formulaic, it's not binary.
11 It is not just one thing. It is not something that you can
12 easily identify.

13 This also means, in the national security
14 community, hiring people who are actually interested in these
15 types of issues and are not just generalists who are assigned
16 a file as they transit a particular operational area. Today
17 you're working in foreign interference, tomorrow you're
18 working on terrorism, tomorrow you're working on something
19 else.

20 It also means, for example, that CSIS
21 intelligence officers who traditionally spent time in
22 communities talking to representatives of diaspora, talking
23 to community leaders, talking to people who understood and
24 represented certain perspectives, this was done in the past.
25 The Service has gotten away from doing that. There is less
26 and less contact with representatives in diaspora
27 communities. I think we need to get back to that model.

28 There's a -- there's reasons for this. We're

1 all aware that after 9/11 and the emergency measures that
2 arose and excesses that are well documented sent a chill
3 through the community. This coincided with an erosion of
4 public trust in government institutions in general as a
5 result of divisive and partisan politics fueled by conspiracy
6 theories and enabled by the media and the internet. And this
7 severe chilling of CSIS officers spending time in communities
8 has had an effect on understanding what is actually
9 happening.

10 The purpose of intelligence service is to
11 give some forewarning and to understand the threat
12 environment. If you're not engaged with that threat
13 environment, you're not going to understand it. And you're
14 not going to understand it by Googling these issues. This is
15 a person-to-person type of phenomena, and those personal
16 relationships are vitally important.

17 I think we can -- notwithstanding the
18 excesses, the issues of the past, we can get back to that
19 model again and have more engagement with communities, if
20 it's done respectfully, if it is done mindfully to
21 constitutional freedom of speech and all those issues, but
22 somehow -- and it is being done with a more diverse
23 population of intelligence officers than in the past.

24 But if you do not have that level of
25 engagement with communities, you're not going to understand
26 what is happening and there will not be a level of trust for
27 members of ethnic communities and diasporas and others to
28 come forward and say that they have been subject to foreign

1 interference and when they call, someone has to answer the
2 phone. Someone's got to talk to them. Someone has to be
3 able to understand what they're saying and why, and how to
4 respond.

5 Short version is that foreign interference at
6 its core is a person-to-person problem. Yes, it's enabled
7 through technology and there are technological approaches to
8 social media and anti-harms legislation and others, but CSIS
9 officers need to get back in the street and do what an
10 intelligence service should do, which is to understand the
11 threat environment at an expert and personal level.

12 I have a deeper example of this, but I'll
13 keep that aside for questions later just in the interests of
14 time.

15 Greater engagement by government and agencies
16 is not without potential controversy. I think we all
17 recognize that. But acts of violence can't be the only
18 starting point for engagement. We can't wait until things to
19 get to a crisis level before there is a government response
20 and response by agencies essentially just acting as
21 spectators rather than trying to predict and counter.

22 Countering divisive messages require active
23 messaging campaigns, and I -- when I'm looking at the foreign
24 interference, I'm reminded very much of the terrorism threat
25 in the early 2000s in dealing with radicalization and how the
26 government was trying to develop effective approaches to deal
27 with radicalization messages on the internet and in another
28 forum and the extreme hesitancy and aversion to dealing with

1 civil society, dealing with ethnic communities, on how you
2 have that conversation about where legitimate freedom of
3 speech, freedom of religion ends, and radicalization begins.

4 I don't think we've sorted that out entirely
5 yet. I think there's still a lot of work to do in that area.
6 There's a very similar issue within the foreign interference
7 domain.

8 Disclosure is a very complex, you know,
9 issue. And when we talk about intelligence-to-evidence and
10 others, but public disclosure of more information in
11 illuminating these threats is extremely useful.

12 The U.S. has pioneered, somewhat, laying
13 charges against foreign actors, even though they know the
14 likelihood of arrest is almost zero. But the process of
15 laying the charge, the information that comes out in court,
16 the description of why the charges are being laid has been a
17 very, very useful mechanism to expose foreign interference.
18 As I said, the charges laid against this Iranian general,
19 against the threat against Ms. Alinejad, the likelihood of
20 him being arrested is extremely low, but the fact that the
21 charges can be laid, and the affidavit, and the court
22 documents explain exactly what their methodology is, what
23 their objectives were, what they've done, and who the victims
24 were. That is a tool that I think is useful -- can be useful
25 in Canada as well, the laying of charges.

26 And I know that there's a -- in a prosecution
27 service, there has to be a likelihood of success in a
28 prosecution, and if you're -- you know, you're -- the person

1 you're laying charges against is on the other side of the
2 world, and probably you're never going to reach them, the
3 likelihood of success is low, but there is a value in that
4 process of revealing that information.

5 There's also concept of strategic disclosure,
6 where a decision is made to reveal sensitive information
7 about a threat where a balance is struck between the loss of
8 secrecy versus the benefit of disclosure.

9 Very rare in Canada do we use this approach,
10 perhaps in part because we are so reliant on strategic
11 intelligence coming from allies who own the rights to it in
12 the first place, but the -- those types of decisions are not
13 going to be made at the agency level. They're going to be
14 made at very senior levels, as to taking in the full opinions
15 of everyone involved, yes, if this intelligence is revealed
16 publicly, there will be perhaps damage or some erosion to the
17 platforms or the ability to gather it in the first place, but
18 the consequence and the benefit of making that level of
19 disclosure may outweigh it for the general -- for the greater
20 good.

21 It's also important to bear in mind that our
22 foreign interference challenges are shared by our closest
23 allies, and therefore we have an opportunity to pursue a
24 common strategy with allies in countering foreign
25 interference.

26 As I said, the U.K., Australia, E.U., U.S.,
27 have all named foreign interference as a growing threat to
28 their democracies. We've all identified the same --

1 primarily the same adversaries and the same methodologies as
2 the source of threat, and so the value of a common cause I
3 think deserves more attention. There is probably more than
4 we can do. As everyone rallied in the post-9/11 to deal with
5 terrorism, there may be considerable advantage in an
6 international forum in dealing with this threat, at least
7 amongst liberal democracies.

8 I'm fond of disclosure, in along the lines
9 that the devil is often in the details. C-70 has got a lot
10 of amendments in it. It's a complex document and I do not
11 even remotely claim to understand all of it or the effects of
12 it. And I don't think even the agencies affected by it
13 entirely understand what it means yet. As with all new laws,
14 when they're rolled out, it takes years of implementation,
15 and court challenges, interpretations, amendments before it's
16 actually fine-tuned.

17 But there's one that stood out to me in the
18 legislation on the registry, Foreign Influence Transparency
19 Registry. In section 15, seems to be a gap, at least to me
20 there's a gap, is that there's a requirement for those who
21 meet the requirements of the legislation to register, and
22 then there will be data holdings and all this. In section 15
23 of that Act, it talks about the disclosure of that
24 information, and it can only be disclosed in the context of
25 investigation of a violation of the Act.

26 There is nothing in it that allows that
27 information, that data, to be accessed by CSIS or the RCMP in
28 the context of a broader foreign interference investigation.

1 It seems counter-intuitive to me to have what is described as
2 a tool in dealing with foreign interference, where the data
3 holdings in it do not appear to be available to the
4 intelligence service, which has written in its mandate to be
5 -- which is to investigate foreign interference, or to the
6 RCMP, which has national security investigations and requires
7 intelligence.

8 There is, in section 17, where it says that
9 the evidence used in a prosecution under that Act can't be
10 used as evidence in another prosecution, this makes sense in
11 a legal sense. I understand that. But the disclosure of
12 that information as intelligence is not going to be used as
13 evidence. It's not going to end up in court.

14 I could get into if, you know, as we go into
15 this, examples of what I mean by that, but my experience is,
16 if a piece of legislation does not explicitly say that that
17 information can be accessed by CSIS or the RCMP for its
18 investigations, or does not explicitly have a mechanism which
19 would clearly allow CSIS or the RCMP to fall under that
20 mechanism, then the policy interpretation is going to be if
21 Parliament intended for CSIS to have access to this, it would
22 have said so, but it didn't, so you can't have it. There are
23 any number of pieces of legislation that seem to fall -- that
24 I've seen that develop over the years.

25 So I'll leave it out there. Legal scholars
26 much smarter than me may understand this better and have a
27 solution to this, but I just wanted to put that down as
28 something that perhaps you could deal with earlier.

1 Another issue which has been alluded to a bit
2 is what I call the compression of the intelligence collection
3 timeline, which has happened over years as the threshold for
4 intelligence investigations and investigative powers to be
5 used increasingly nears criminal evidence levels, that
6 there's been -- and I've watched this happen over literally
7 30 years, of where an intelligence investigation is supposed
8 to start early and be contained under constitutional
9 restrictions within law as to what the results of what that
10 intelligence investigation is used for, is the threshold to
11 authorize those investigations to use the power has slowly
12 crept up towards what the police would have to meet under a
13 criminal investigation so that the product that is being
14 collected is creeping towards being viewed as criminal
15 evidence.

16 What that has been doing is moving the
17 timeline what I would call to the right, and that time for
18 forewarning is getting shorter and shorter as you continually
19 aren't able to start the intelligence collection earlier.

20 I'm not sure if this is intentional. It
21 might be. It may be the result of 30 years of jurisprudence,
22 and laws, and changes in policy interpretations, but you
23 could certainly feel it in investigations where you just
24 don't have on ramps, what I would call on ramps to
25 investigation, which years before you write it, the on ramps
26 don't exist. You're expected to somehow start well down a
27 line to almost an evidentiary level before you can get the
28 authorities you need to gather intelligence to get

1 forewarning.

2 The, you know, issue of intelligence-to-
3 evidence is relevant to the foreign interference
4 investigation. I'm not going to go through that. I think
5 we've talked about that quite a bit.

6 But I will talk about disclosure, and
7 something that as I was preparing to speak to you today that
8 I just happened to come across, which is on the MI5, the
9 British Security Service's website. And it says -- and I'll
10 -- some of it will be quote, some of it is just to set it up,
11 is that an incoming Prime Minister will be told about any
12 information it may have about a potential Cabinet Minister
13 that raises a serious national security concern and only if
14 it appears likely that the individual concerned will need
15 access to sensitive information. The site goes on to say:

16 "A similar arrangement has been in
17 operation for the Official Opposition
18 since 1992. The Leader of the
19 Opposition is briefed on any serious
20 security issue concerning a possible
21 member of the Shadow Cabinet. This
22 is necessary because members of the
23 Shadow Cabinet are often briefed on
24 security issues."

25 I found that to be an interesting piece in
26 the context of some of the discussions -- a lot of the core
27 discussions around the Commission, is that clearly others
28 were thinking about these issues and have ways of approaching

1 it. I don't -- I can't tell you what exactly happened in
2 1992 that is referenced on there. I know that around 1992
3 the UK authorities passed significant legislation around
4 terrorist threats, which were building in the UK, so it may
5 have flowed somehow out of that. But I think it may be
6 something worth looking at to see what is behind that
7 approach and why do they -- and it sits right on their
8 website, in a public website to address.

9 On the broader issue of the effectiveness
10 that Canadian national security apparatus -- Mr. Jean
11 discussed this in detail. I don't want to repeat it, but I
12 just think from a practitioner's perspective at times, there
13 was a sense that the approach to national security was very
14 uneven in Canada, even what national security is, it's kind
15 of an amorphous definition at times, but the approach seemed
16 to be uneven, particularly as you went from government to
17 government. That's the right. But that continuity and the
18 ability to follow an issue over a period of years where these
19 issues are often perennial, in 1997 -- 1987, I worked on the
20 investigation of foreign interference in Canada by the
21 Government of India. Thirty-seven (37) years later, we're
22 still talking about it. So the ability to track these issues
23 over time and deal with them may have in part a structural or
24 a systemic problem in Canada if we do not have -- and I don't
25 want to say that we should do what the Americans do, have a
26 National Security Council, but a National Security Council is
27 somewhat different than the functions of the -- for example,
28 the Privy Council Security Intelligence Secretariate, which

1 is the Secretariate the Cabinet functions. They have
2 different objectives, they have different staffing levels,
3 and they have different continuity. And many times over the
4 years I would deal with representatives from the United
5 States, from the United Kingdom and often Australia at senior
6 Public Service levels, who had been working these files for
7 years, and the Canadian representatives had been kind of
8 moved in quickly to deal the file as just one of the many
9 issues that they had to deal with on their plate. And there
10 seemed to be a lack of a structural approach to this, which I
11 think may have some knock-on effects to some of these broader
12 issues.

13 With that I'll end my comments and happy to
14 take questions. Thank you.

15 **COMMISSIONER HOGUE:** Thank you.

16 **DR. LEAH WEST:** Thank you very much.

17 Professor Carvin?

18 **--- PRESENTATION BY/PRÉSENTATION PAR DR. STEPHANIE CARVIN:**

19 **DR. STEPHANIE CARVIN:** Thank you. So I kind
20 of went question by question process. So does Canada -- do
21 Canadian intelligence agencies have the legal authorities,
22 technical capabilities and resources necessary. I think
23 there's broad consensus on this panel that most of the legal
24 authorities are there. This is not a problem of law. This
25 is now a problem of enforcement, making policies, review
26 practices, all of this kind of thing. I will make two
27 possible observations, perhaps in direct opposition to the
28 very passionate discussion by Lex, which I very much agree

1 with, but one of the things I noticed about our foreign
2 interference transparency registry is that it looks at
3 sectors that lobby the government, right, the political
4 level. It does not look at other institutions like the
5 media, and that is such a third rail to touch. But I would
6 note that, you know, the recent reporting out of the United
7 States, which, allegedly -- I emphasize allegedly -- may
8 reflect Tenet Media, there's foreign interference -- you
9 know, there's clearly foreign states that want to impact
10 media, the way it's perceived and things like this. Do we
11 need to think about that in terms of our legislation, or are
12 there other mechanisms we can do?

13 The other issue I wanted to just touch on
14 briefly because I do think it's a whole can of worms that is
15 outside the scope of this particular conversation, but the
16 intelligence-to-evidence issue was not addressed in Bill C-
17 70, and I do believe it continues to be a missing piece of
18 the legislative puzzle and should be addressed in the future.

19 On the issue of recruitment, retention and
20 training, I do have concerns about the capacities and
21 resources. I don't think I need to go over the multiple
22 reports. I believe there's now been 10 on RCMP policing, and
23 the fact that they are simply unable -- and Mr. Jean said
24 that fairly importantly, I think, but the fact is that the
25 contract policing is really inhibiting national security
26 investigations. So, you know, I don't want to get into this
27 issue further, but just to note that I think it's one of the
28 largest structural issues that we actually have.

1 The point that I think Lex made about, you
2 know, diaspora groups contacting the police about their
3 concerns, and then nothing happening, or them not being aware
4 of the situation, or questions of jurisdiction I think
5 somewhat tie into this.

6 But I also have similar HR issues about the
7 intelligence community at present. As far back as 2018 as
8 part of a research project, I interviewed someone who worked
9 in the community who said their organization identified
10 recruitment as one of their top challenges, and this has only
11 gotten worse in the years since. There's budget cuts, a
12 paralyzed -- the security clearance process to me in the last
13 year has been described to me as completely paralyzed; right?
14 This is huge. It can take up to two years. There's
15 retention issues that's seriously hampering the ability for
16 the community to do its job.

17 And I don't know to the extent that, like,
18 very specific HR practices are going to be a part of your
19 final recommendation, but I do note that if you do not have -
20 - or if you have a burned-out community because you can't
21 replace people, there's insufficient staffing, if people are
22 acting in more than one position for periods of time, this is
23 ultimately going to impact our ability to do the job.

24 And then both the RCMP and CSIS, to a certain
25 extent, have a generalist model, right, in terms of their
26 recruitment. You know, if you're in the RCMP, you show up at
27 Depot, you do your training there, and then you go off and
28 work in, I don't know, murder investigations in Newfoundland

1 for a long period of time, and then you may be brought onto a
2 national security investigation, and then you probably work
3 there for a couple years, and then you're back to the
4 province. I do worry that -- you know, we've all talked
5 about the fact and, you know, Mr. Jones just said I think
6 really well that there's this issue of focus, and he referred
7 to a National Security Council. But I also think, like,
8 allowing individuals to develop specializations like they do
9 in other Five Eyes countries would be a good idea. We need
10 less of a generalist model. And the ability for people to
11 develop that expertise over a period of time.

12 The second question is what measures can be
13 taken to make the relationship between Canada's intelligence
14 agencies and government policy makers effective and more
15 efficient. So I wrote a book on this, so I can't submit the
16 book, I don't think. It wouldn't really be fair ---

17 **COMMISSIONER HOGUE:** I've read it.

18 **DR. STEPHANIE CARVIN:** Oh, wow, there you go.
19 Okay. So impressed. Awesome. That's going in the promotion
20 file.

21 And I wrote it with my friend Thomas Juneau.
22 Basically, to summarize, we conclude that intelligence
23 literacy in the policy community remains low. You know, the
24 courses that are being developed at PDI, University of
25 Ottawa, are trying to solve this challenge, and Mr. Jean as
26 well, are working on that. But a lot of times individuals
27 would talk to us about the intelligence being in a black box,
28 not knowing how it was made or where it was coming from. And

1 there's also a sense that the policy community needs to
2 improve -- sorry, the policy community needs to improve its
3 strategic understanding to understand what the roles of the
4 different departments' agencies are in our national security
5 process.

6 Like it or not, and there's a lot of reason
7 not to like it, but, you know, I tell my students now, I'm,
8 like, if you want to fight espionage and foreign
9 interference, go work at ISED, go work at Innovation, Science
10 and Economic Development Canada, right, because they have the
11 *Investment Canada Act*. This is one of the most powerful
12 pieces of legislation we actually have. So we need to make
13 sure that all these departments and agencies know their
14 roles, responsibilities and limits.

15 But also, policy literacy is lacking in the
16 intelligence community, and I think to a certain extent it's
17 true that intelligence agencies, managers, analysts do not
18 understand their clients and do not understand their
19 priorities as well as they should, and this means products
20 are crafted in ways that don't speak to them, or are too
21 long, or are not timely. And it is a good thing that there
22 is tension in the relationship. There should be -- someone -
23 - you'd mentioned challenge function. You know, we want that
24 challenge function to be there, but that's going to -- so I'm
25 not saying there should be, like, perfect harmony between the
26 two communities. I don't want that at all, but I think that
27 two communities that understand each other better are going
28 to have that more dynamic relationship. That challenge

1 function is going to function better and produce better
2 products. And I think that some of the steps that could be
3 taken would be to better train analysts to produce contents
4 that better spoke to their clients. Certainly, our client --
5 I think our Five Eyes partners do a better job with this than
6 we do.

7 And secondly, we need to do a better job of
8 utilizing secondments in our national security agencies and
9 in our policy communities. Right now, I mean, I'm going to
10 be blunt and just say secondments are used to get rid of your
11 worst employees. And it's, like, who can I get rid of for
12 two years? Oh, this person. Great. That's not the way it
13 should be. It should be our best employees that are being
14 put forward to learn about other communities, so that when
15 they come back, the relationship will hopefully be better.

16 And we need to find ways to make it easier
17 for policy analysts and their senior clients to access
18 classified information. You know, we heard -- if I followed
19 the news correctly, there were challenges in getting certain
20 Ministers classified information during the pandemic. But
21 right now, even just accessing a SKIF, like the classified
22 information facilities is hard. You have to leave all of
23 your -- you know, you're a Deputy Minister. You have to
24 leave all your electronic devices behind. You're being
25 pulled away from any other ---

26 **MS. LEILA GHAAHARY:** Ms. Carvin? Excuse me
27 sorry.

28 **DR. STEPHANIE CARVIN:** Am I speaking too

1 fast?

2 MS. LEILA GHAAHARY: Yes, please could you
3 slow down?

4 DR. STEPHANIE CARVIN: I'm sorry.

5 MS. LEILA GHAAHARY: Thank you.

6 DR. STEPHANIE CARVIN: Pity my students.
7 Thank you. I am sorry.

8 Anyways, so they have -- once they have this
9 information, you know, they're pulled effectively from their
10 -- all their -- everything that's on fire, and then they're
11 having to read this information, find it on a computer that
12 was probably from 2008 and takes like 10 minutes to start up,
13 and once they have this information, it's difficult for them
14 to share what they know, even if they can act on it.

15 We need better coordinations of our
16 institutions. We need to -- we need to do a better job of
17 feeding intelligence up the chain. That's probably one of
18 the biggest themes coming out of this entire Commission.
19 This was also found in the Johnston report, which found the
20 government is missing effective protocols on information
21 sharing, intelligence gathering, and distribution.

22 I'm pleased to say that I think there have
23 been steps taken to improve this recently. There's more DM
24 and ADM committees, there's now a Cabinet committee, although
25 I agree it's way too early to say if it has or hasn't been
26 effective at this point.

27 Then this brings us to the interesting
28 question, the NSIA, and whether that office should be

1 strengthened.

2 I'm sympathetic to the view that, you know,
3 maybe legislation is not going to be the perfect fix, but I
4 do believe the NSIA needs a better and bigger staff and -- or
5 at least a secretariat, and that there should be at least
6 some kind of entrenching of the functions of the ability to
7 coordinate the intelligence community in Canada.

8 One of the things we found in our book, the
9 one I wrote with Thomas, Thomas Juneau, is that a lot of the
10 community in Canada is personally driven. It's driven by
11 personalities, and when those personalities move, some of
12 those initiatives can be lost. So the more I think we
13 actually entrench some of these ideas, whether through
14 legislation, or far clearer policy directives, or something
15 like that, I think for the better.

16 So I kind of lumped under our section
17 questions three, four, and five, and I'm just going to talk
18 briefly about two things. One is open-source information,
19 and secondly, learning to communicate better with affected
20 communities.

21 On the issue of open-source, I think this is
22 actually one of the best ways that we can actually -- you
23 know, this challenge of information sharing. If we can do a
24 better job of open-source, I think that this would take care
25 of a lot of our problems.

26 You know, like Thomas and I -- I should say,
27 Thomas Juneau and myself have -- we estimate that somewhere
28 between 70 to 80 percent of classified information probably

1 is available in open-source somewhere; right? That's not a
2 perfect measurement, but certainly this information could be
3 used to communicate with those without clearance. There was
4 actually really good steps taken on this during the pandemic;
5 right? Where people couldn't actually access their
6 classified information, so there was kind of a flourishing of
7 open-source products, which was really good.

8 But basically, Canada needs a centralized
9 body with a mandate to collect -- I appreciate that some of
10 my colleagues have challenged the need for new institutions,
11 but hear me out.

12 Canada should have a more, let me say
13 centralized approach, to collect open-source information from
14 across the Canadian intelligence community to maximise the
15 potential of modern OSINT collection, tools, and products.
16 To be effective, the body needs to have the mandate to
17 develop and share OSINT across all levels of governments,
18 become a federal policy leader and centre of excellence for
19 OSINT collection, training, and analysis, and I appreciate
20 there would be significant legalities and legal processes
21 needed around this too, and could work to improve the
22 coordination and breaking down of current OSINT silos. Right
23 now a lot of the agencies out there do do some kind of OSINT,
24 but it would be great if we could kind of unite this
25 together, and it would enhance Canada's OSINT culture and
26 capability.

27 And I should say that Professor West and
28 myself, we have a chapter coming out in -- I'm really just

1 using this platform to promote my work. Sorry. But
2 basically the Integrated Terrorism Assessment Centre might
3 actually be the appropriate body to do this. I think ITAC,
4 it would be -- especially since it was originally created
5 with this mandate of doing more interaction with front-line
6 communities, and that would be impossible -- that would be
7 possible to do under an enhanced NSIA role or office,
8 discussed earlier.

9 And the final thing I'll talk about is
10 learning to communicate with effective communities.

11 You know, we're doing this at a time -- this
12 conversation at a time when I do want to note that hate
13 crimes against Asian Canadians, and I would say Indo
14 Canadians and South Asian Canadians, have surged.
15 Particularly in the wake of COVID-19, and sensitivity to this
16 reality is important and needs to be reflected into
17 operations of those institutions taxed with combatting
18 foreign interference. It needs to be at the heart of our
19 understanding.

20 We can't -- I don't think we should approach
21 foreign interference out of fear. I think we need to do it
22 out of empathy; right? And from the view of the communities
23 that are primarily effective.

24 Unfortunately, the generalist model that I
25 discussed earlier used in the national security communities
26 with the lack of specialists within these organizations may
27 be hampering outreach, although, you know, I take all the
28 points made by Mr. Jones as well.

1 Often, you'll find, you know, the roundtable
2 approach. "Hey, everyone, come together. We're going to
3 talk about foreign interference in communities." That's not
4 going to work if people are terrified to speak out.

5 So, you know, we have to find ways to reach
6 communities in ways that people who do speak up are not doing
7 it in front of everyone else, that you do have these secure
8 ways of managing these issues.

9 And I also take very much Lex's point that
10 the communities themselves don't understand the institutions
11 that are out there. It doesn't help in our very federal
12 system when you have someone reach out for help and, you
13 know, you call CSIS and CSIS says, "Thank you for the
14 information. There's nothing we can do. Contact the RCMP."
15 The RCMP looks at it and then says to contact your local
16 police. And you contact the local police and they're not
17 being briefed on any of this, so they don't understand the
18 global context, right, and just say, "Well, there's nothing
19 really we can do." I can't imagine a more alienating
20 feeling.

21 We need to take care when we're crafting
22 materials to do outreach to these communities. We can't just
23 ChatGPT our documents into Chinese and literally translate
24 them and expect that you're capturing the nuances of all the
25 language. So we need to actually hire people who understand
26 these communities, who speak the language, ensure that we are
27 taking care when we're translating the documents that we're
28 putting out there to reflect the nuances of languages and

1 customs.

2 And then finally I'll just say, to the point
3 of community engagement, that there's been a lot of criticism
4 of the community and the way it engaged with diaspora
5 communities, particularly the Muslim communities in the post-
6 9/11 era, and I don't know if we've done a good job of
7 listening to what those concerns actually were. And for the
8 reasons -- some reasons that Mr. Jones mentioned, but
9 practices like just kind of showing -- door knocking, showing
10 up at places of employment, these were highly criticized
11 practices, and I don't know to the extent -- you know, as
12 we're right now realizing we need to re-engage with these
13 communities, I don't know if we've done it with a view of
14 learning the lessons of the past two decades of
15 counterterrorism. We need to, like, actually reflect on what
16 happened, figure out, you know, are there better ways of
17 engaging with these communities than just kind of showing up
18 and knocking on the door? Sometimes I feel like IOs only
19 kind of have one method of engagement, which is the door
20 knock approach, and I think maybe we could do better.

21 So let's take these concerns, especially
22 those raised by, you know, the Muslim community, the Sikh
23 community in the wake of -- you know, during the passage of
24 C-70, seriously, or else I take the point there's just not
25 going to be sufficient trust to communicate with these
26 communities as we go forward and try to address this problem
27 of foreign interference.

28 Thank you.

1 COMMISSIONER HOGUE: Thank you.

2 DR. LEAH WEST: Dr. Robson-Morrow?

3 --- PRESENTATION BY/PRÉSENTATION PAR DR. MARIA ROBSON-MORROW:

4 DR. MARIA ROBSON-MORROW: Thank you very
5 much. Thank you, Madam Commissioner. Thank you, fellow
6 panellists. And to the Commission for the invitation.

7 I do need to note right off the bat that the
8 views expressed here are my own and not those of my employer.

9 I also want to do a time check. May I still
10 take approximately 12 minutes or should I try to ---

11 DR. LEAH WEST: No, take as long you ---

12 DR. MARIA ROBSON-MORROW: --- leverage my ---

13 DR. LEAH WEST: --- have prepared for.

14 DR. MARIA ROBSON-MORROW: Thank you. So I
15 have two core arguments, underlying principles, for my
16 remarks today that I believe will align with what my
17 colleagues have said.

18 The first one is, as Mr. Jean mentioned, the
19 Crown Jewels are not all in the hands of government. They're
20 certainly not all in the hands of the national security
21 agencies. And Canada's national security apparatus must
22 provide mechanisms for effective trusting two-way engagement
23 with external parties. And critically important, this
24 national security apparatus must treat these parties as
25 potential partners, not just victims. They have pieces of
26 the puzzle as well. We're not just there for one-way
27 directional briefing to them. It has to be an engagement.

28 Second is that we are not the only ones

1 facing these challenges, and as Mr. Jones mentioned, our
2 allies, particularly our intelligence sharing partners within
3 the Five Eyes have a lot of models, they're tackling this as
4 well, that are relevant when applied in a Canadian context.

5 So I will have those two underlying
6 principles or arguments here, and my remarks are structured
7 in three different categories of engagement.

8 The first one is duty to warn or duty to
9 advise. The second one is engagement models with external
10 parties that focus specifically on foreign interference. And
11 the third is engagement models writ large with a security
12 focus, but not necessarily foreign interference, but they
13 have characteristics for successful engagement that are
14 relevant for us for the purposes of the Inquiry and the
15 Commission.

16 And for this one, I'll be drawing on eight
17 years of research and, like Professor Carvin, interviewing
18 practitioners in the community and drawing lessons from their
19 experiences.

20 So the first category of engagement is duty
21 to warn or duty to advise.

22 Most of the Five Eyes countries do not have a
23 formal duty to warn. It rests within law enforcement
24 entities, so the RCMP has its obligation here.

25 We see this across the Five Eyes. The
26 country that does have a formal duty to warn for the entire
27 intelligence community is the United States, with
28 Intelligence Community Directive 191, and it's a relevant

1 model for us to look at.

2 It focuses on threats to life. However,
3 there are aspects of the directive that I'll posit today are
4 relevant for us when thinking about potential duty to warn in
5 a foreign interference context.

6 The directive is very specific, and it's
7 available to the public. It's online. It's slightly
8 redacted, but most of the content is available. And it
9 stipulates that any intelligence agency in the United States
10 that collects or acquires credible and specific information
11 indicating an impending threat and, in this case, it's to --
12 it's for intentional killing, bodily injury or kidnapping --
13 directed at a person or a group of people shall have a duty
14 to warn the intended victim or those responsible for
15 protecting the intended victim as appropriate.

16 And there are a few salient aspects of the
17 directive, including the fact that it's to warn those
18 responsible for protecting, not just the victim themselves.
19 Also, it explicitly states in the directive that tear lines,
20 so the information that's shared must omit information that
21 would compromise sources and methods. This goes to the
22 intelligence evidence problem.

23 But what's important here is that Directive
24 191 is frequently acted on. This isn't a crutch to avoid
25 warning. Rather, the expectation is warning shall be done,
26 so we must do it in a way that protects sensitive
27 information.

28 It also does clearly stipulate that warning

1 can be waived under certain conditions, and I think this is
2 really important. It goes into details as to why warning
3 might not be possible. And to me, that's critical because if
4 we discount the possibility that warning might not be
5 feasible or there might be a very, very good reason not to
6 warn, then it invites non-compliance because there will
7 always be cases in which warning can't be done. But what we
8 see with Intelligence Community Directive 191 is that, often,
9 it is done.

10 There is warning with a risk calculation,
11 with appropriate safeguards in place, so that's why I think
12 this directive is an interesting model for us to look at.

13 So what we see here in Canada with C-70 is an
14 open-ended ability to warn with flexibility. That's
15 important, but also, with flexibility and open-endedness can
16 come some confusion and even the potential for preferential
17 treatment, so this is where having some specificity can
18 actually help avoid some outcomes we might not want.

19 The other piece of relevant literature in
20 Canada I want to point to on the legislative is the directive
21 -- Ministerial direction from the Minister of Public Safety
22 in May of 2023 regarding threats to the security of Canada
23 directed at Parliament and parliamentarians, which requires
24 CSIS to ensure parliamentarians are informed of threats as
25 well as working through the RCMP, law enforcement agencies
26 and other departments.

27 So there is a requirement here, but it is not
28 as specific, so again, there's some value in flexibility. We

1 heard about interpretation. However, our partner countries
2 do have some models that have these guardrails or these
3 specifics in place that can be useful. So that's duty to
4 warn.

5 The second category is engagement with
6 external parties specific to foreign interference. And Mr.
7 Jones has mentioned a bit of this, so I'll go into a few
8 details that will be similar and build on what you mentioned.

9 We were asked on the panel whether and how
10 Canada's national security and intelligence agencies should
11 communicate with the public on foreign interference. And my
12 answer is yes, they should, and there are models within our
13 allies and partners as to how this can be done, recognizing
14 this is very nascent and no one has all the answers and
15 they're still figuring it out.

16 So Australia and the United States both have
17 these centres that have been established to tackle foreign
18 interference and to share externally. Australia established
19 their counter foreign interference coordination centre back
20 in 2018, and this supports the National Counter Foreign
21 Interference Coordinator. And I know the panel yesterday
22 actually discussed the potential for a coordinator, so there
23 is a model in Australia that's a few years old that is, as we
24 heard, relevant for us to look at here.

25 The centre has a whole-of-government approach
26 and it also, critically importantly for us, works with the
27 private and civil sectors, the wider community and
28 international partners to strengthen Australia's response and

1 resilience to foreign interference. It includes a hotline.
2 As we heard from Professor Carvin, a hotline is not
3 necessarily the answer. It depends how it's used. But there
4 is this track record in Australia of use. We could talk to
5 them about it. But also, two-way engagement with external
6 parties.

7 In the United States, the equivalent is the
8 Foreign Malign Influence Center within the office of the
9 Director of National Intelligence, which was activated in
10 2022. And the center was established because of a
11 recognition, and this goes back to what Mr. Fadden said at
12 the beginning, about the idea that foreign interference
13 targeting democratic processes is not just in the context of
14 elections. It's 365 days a year. It's every year, there
15 needs to be an ongoing model, and so that was the basis for
16 establishing a permanent centre.

17 There are two aspects of the Foreign Malign
18 Influence Center that I believe are important for us. The
19 first is that it's not just for internal assessments of a
20 threat. There is a public notification protocol that is
21 really emphasized as part of their mission activities,
22 notifying victims and, when appropriate, the public through
23 advisories.

24 And there's risk calculation to ensure not
25 just that sensitive information sources and methods are
26 protected, but also that notification doesn't do the work of
27 the adversary, that it doesn't actually amplify the messages
28 of foreign interference. And that's explicit in the

1 documentation of the Center.

2 And then the second key aspect is that one of
3 their key pillars is external engagement, including
4 information exchanges, so it's not just about pushing
5 information. It's really about engaging, recognizing, again,
6 that the pieces of the puzzle are not all in the hands of
7 government. They're also in the hands of external parties,
8 civil society, government partners and industry.

9 So I mention these two models again to say,
10 as Mr. Jones said, that our allies are attacking similar
11 challenges in their models that are relevant for a Canadian
12 context.

13 The final category is engagement models writ
14 large looking at security issues and key characteristics in
15 them that can lead to success. And one of the exemplary
16 models here is the U.S. State Department's Overseas Security
17 Advisory Council.

18 This is an organization that's existed since
19 1985 with a mission to promote security cooperation by
20 fostering a global network of security professionals who
21 exchange timely information and security best practices. And
22 although it focuses on industry, it also includes non-
23 profits. It includes those who have pieces of the threat
24 picture, and it's been very adaptive over time to include
25 those who have pieces of the puzzle.

26 It includes Canadians, Australians, French
27 members and others who all have some relevance for the
28 security of U.S. persons.

1 And this model came up at a Public Safety
2 funded study conducted by the Conference Board back in 2017
3 that asked how Canada could improve information sharing
4 between the government and non-governmental parties. The
5 report has a lot of relevance to what we're talking about
6 today, and it was -- they surveyed Canadians. There were
7 recommendations for Canadians about Canadian institutions,
8 and yet they mentioned the State Department's Overseas
9 Security Advisory model as a model that has relevance for us.

10 The Australians also took note of this model
11 and they went to the Overseas Security Advisory Council,
12 learned from them and built their own institution called ASIO
13 Outreach. It's the Australian Security Intelligence
14 Organization Outreach branch which sits within the
15 intelligence agency but has an external engagement remit and
16 has productive conversations with businesses and civil
17 society on security questions.

18 So both of these models recognize that there
19 are external parties who want to engage who have pieces of
20 this puzzle.

21 So what are the keys for engagement? And
22 this is how I'll wrap up my discussion.

23 The successful models like the Overseas
24 Security Advisory Council, they build trust. As Mr. Jean has
25 mentioned, there's a need for a culture of engagement that
26 goes beyond just what the law permits, but actually what
27 organizations seek. And the Overseas Security Advisory
28 Council model, the agenda is driven by the external parties,

1 not just by what the government believes they want to hear.

2 The external members actually help set the
3 agenda, determine the priorities that are tackled, and that's
4 part of their success.

5 So to conclude, I have four key
6 characteristics that I've noticed across these different
7 models for effective external engagement.

8 The first one is repeat interactions when
9 possible, not one-offs. Repeat interactions build
10 credibility and build trust. That's number one.

11 Number two is two-way interaction. So
12 defensive briefings have a role to play, but two-way
13 engagement, again, builds more trust, adds more value and
14 many of my research interviewees expressed dismay at being
15 briefed one way and not being able to share back because they
16 actually did want to share back.

17 The third is building mutual understanding.
18 This was a key theme of -- in my interviews, was it's
19 important to foster knowledge of each other's knowledge,
20 capabilities, priorities and pain points. This leads for
21 better information exchange. Understanding what the
22 government can or can't do, can or can't share, can or can't
23 actually collect is really important.

24 This may not apply to briefing policymakers
25 on specific threats, but it definitely applies for engaging
26 civil society, industry and diaspora groups.

27 And then the final one, number four, is when
28 possible, leveraging already existing organizations. There

1 are recent studies that talk about the erosion of trust in
2 federal institutions, but the endurance of trust in local
3 institutions and local government and civil society groups,
4 industry groups, and the Public Safety funded study by the
5 Conference Board that I mentioned, they talk about this focus
6 on associations, pre-existing organizations, is more trusted
7 than government, and when government engages through those
8 groups to the extent possible, that results in a more
9 productive dialogue and engagement, and this goes to the
10 point by Mr. Jean about horizontal networks of engagement as
11 well being really important.

12 So to conclude, effective engagement includes
13 external parties who have pieces of the puzzle. They're not
14 just there to be briefed. It has to be two-way. They often
15 do want to engage, but as we've heard, it actually has to be
16 a genuine engagement. And our partner countries have models
17 that are instructive and have some value when we look at them
18 in a Canadian context.

19 Thank you.

20 **COMMISSIONER HOGUE:** Thank you.

21 **DR. LEAH WEST:** Thank you. I think this will
22 bring us to the end. We'll take a break.

23 **COMMISSIONER HOGUE:** Yes. And I will say
24 there's a lot to look at, so we'll take 30 minutes, but we'll
25 be together. We'll be able to review questions received from
26 participants and then we'll come back. So roughly we should
27 be able to resume at 11:10/11:15.

28 --- Upon recessing at 10:39 a.m./

1 --- La séance est suspendue à 10 h 39

2 --- Upon resuming at 11:26 a.m./

3 --- La séance est reprise à 11 h 26

4 **COMMISSIONER HOGUE:** We have a lot to
5 discuss, so I suggest that we start right away.

6 **--- OPEN DISCUSSION/DISCUSSION OUVERTE:**

7 **DR. LEAH WEST:** So there are many questions
8 that came in, and so we're going to kind of group them
9 thematically.

10 And one of the first things actually harkens
11 back to what Mr. Fadden started off with, which is this
12 culture of understanding the threat. Canadians understanding
13 what it is that FI is and who to talk to, and understanding
14 the intelligence that is being put out, and trying to improve
15 that understanding. And so this goes a lot to the education
16 of the Canadian public about this threat.

17 So I'm going to actually ask Dr. Carvin, if
18 you'd like to start, and talk about how the community, the
19 intelligence community, can do a better job of educating the
20 public about this threat so that there is better engagement?

21 **DR. STEPHANIE CARVIN:** Thank you for your
22 question. So there's a number of steps that I think could be
23 taken. First of all, I think better communication depends on
24 better understanding; right? So I think the community itself
25 needs to educate itself on the communities it wishes to speak
26 to; right? There's going to be differences. Even within
27 communities there's going to be big differences. Like, if
28 you're, you know, I don't know if the community has come up,

1 but, like, there's been talk of foreign interference in the
2 Eritrean community. There's a lot of division and
3 differences in that community, and knowing how to speak to it
4 I think is going to be very important.

5 Now, are you going to have someone who is
6 just able to speak that language and do -- it might be asking
7 a lot of a very small community. But there's a lot more that
8 we can do.

9 So secondly, I think it requires
10 specialization. I spoke earlier about the issues with
11 generalists and the need for more specialization. Again, we
12 are a small community. This will be difficult to do. But
13 the community itself needs to find the capacity to develop
14 that expertise within, and that might be perhaps looking
15 outside the normal kinds of areas of recruitment, more
16 anthropology, more -- and perhaps even social work at some
17 point. You know, like, kind of thinking outside the box in
18 terms of how you go and work with these communities I think
19 would be fundamental. And I appreciate that this is a
20 challenge.

21 So those better understanding -- and then the
22 other points I raised in my commentary was the need to craft
23 products that are nuanced, that are in the language of the
24 communities, that you need to take -- that they're not just
25 direct literal translations of those documents.

26 I have spoken to people in the Chinese
27 diaspora, and they're like, "Yeah, we can tell when someone -
28 - when something got put through, you know, ChatGPT or Google

1 Translate." It's not going to cut it; right? Those nuances
2 need to be there.

3 And then finally, there is an issue with
4 regards to how -- the actual means of communication. And I
5 appreciate that, like, you know, there's some talk of doing
6 more reporting and stuff like this. If we generate another
7 200-page report that's available in English and French, yes,
8 some people may read it, but we need to be thinking about
9 better crafted documents, reports, for how we do this, and
10 possibly utilizing new means of communication. I appreciate
11 not everyone agrees, but being able to take the key messages,
12 right, maybe just the key messages and putting those into
13 some kind of video. Not necessarily on the threat. I guess
14 the model I would put out is, that you and I would be
15 familiar with, Professor West, would be the three minute
16 thesis; right? The three-minute thesis is -- you don't get
17 all the nuances of someone's PhD, but they should be able to
18 convey to you the key messages of your PhD in three minutes.
19 That's the idea of that.

20 And, you know, I think that might be not the
21 model, it would a tool in a toolkit that then might help get
22 people to understand what some of these issues are, and then
23 provide access to resources and other pathways that they
24 could learn more about the threats, or perhaps even bring
25 some information that they had forward.

26 **DR. LEAH WEST:** Mr. Fadden?

27 **MR. RICHARD FADDEN:** Thanks. I'd like to try
28 to approach this from a slightly different perspective,

1 although I agree with what Stephanie was saying, except her
2 three-minute specials, but that's for another day.

3 We have to remember that public officials who
4 are operating in all of these agencies actually work for
5 Ministers. And aside from the cultural change issue, there's
6 a real risk aversion on the part of Ministers which has grown
7 tremendously over the course of the last 20 years. And
8 people don't want to take any chances.

9 So one way of encouraging public education,
10 more discussion, would be for the government of the day,
11 whoever forms that government, to clearly indicate that
12 they're willing to encourage this. And if they take all of
13 this seriously, they should do that.

14 The other way of doing this, and I would note
15 that agencies, as opposed to departments, are much more
16 closed than departments. It's harder to change them. And
17 one way of doing it is through the issuance of very, very
18 clear instructions.

19 I'll give you an example. I've headed two
20 agencies, and in one of them, something that had never been
21 done before, they didn't want to do, it was against their
22 professional judgement, I got a call from the Clerk who said
23 he had been speaking to the Prime Minister, blah, blah, blah,
24 blah, and by the time we were finished, a quarter of a
25 billion dollars had been spent with very, very clear
26 instructions that that agency had to do A, B, C.

27 If you tell the head of head of CSIS, the
28 head of CSE, of FINTRAC and whatnot, clearly, unambiguously -

1 - tie their bonus to it if you want to -- that they have to
2 come up with concrete examples of how to communicate, that
3 would go some distance. But I think though that you have to
4 acknowledge that the Commissioner's recommendations in the
5 short-term cannot rely on cultural change. They take time.

6 So I would substitute that with, you know,
7 sort of beating Ministers about the head to be very
8 supportive and issue very clear instructions that you want A,
9 B, C done.

10 One thing agencies tend to do well is if
11 they're given very clear instructions, they tend to obey.
12 And it's a poor substitute for real cultural change, but in
13 the short to medium term, you may actually get some movement.
14 This along with the things that Stephanie's talked about.

15 **DR. LEAH WEST:** Dr. Robson-Morrow?

16 **DR. MARIA ROBSON-MORROW:** Thank you very
17 much. To add a third perspective that tackles a different
18 part of the educating question, we've heard about engaging
19 community elements, engaging diaspora groups. There are so
20 many different threat vectors in terms of how foreign
21 interference can manifest, who the targets are, and so
22 there's a risk in broadbrush approaches. There's public
23 advisories, but often they're not really targeting one
24 particular group and there's a limit to who will actually
25 access them, or be interested in them, or really understand
26 what the message is.

27 But one aspect I wanted to highlight was
28 engaging with universities, because I think this is a really

1 important aspect of the attempts to counter foreign
2 interference in Canada and elsewhere. So CSIS has been more
3 actively engaging. I know Global Affairs Canada also engages
4 with universities on research security. And I know the
5 Commission's focused specifically on democratic processes.
6 But I think it's all interrelated. It's all different ways
7 that adversaries can target our institutions and intellectual
8 leaders and students and so forth.

9 But we mentioned the Australian models
10 earlier, so I wanted to come back to Australia, because
11 Australia, in addition to the Centre we talked about earlier,
12 has a university Task Force that was established in 2019 that
13 engages government that's engaging directly with the
14 universities to try to build this understanding of foreign
15 interference, what it means for research for educational
16 institutions. And so I think that's a relevant model. And
17 also just a broader message of when we think about engaging
18 the public, there are all these different elements to the
19 public to think about.

20 **DR. LEAH WEST:** Just to follow up on that,
21 when you mean they're engaging with universities, is it only
22 on research security, or also to deal with foreign students
23 and the vulnerabilities there?

24 **DR. MARIA ROBSON-MORROW:** I think I'll not be
25 the only one to speak to this, but much broader than just
26 research development and research security. Certainly
27 foreign students, I don't want to speak too much outside of
28 my experience on this issue in talking to practitioners on

1 this issue, but I believe the emphasis on focusing the
2 culture of international students being welcomed and part of
3 the university fabric while still recognizing risks that they
4 might be targeted, foreign interference risks that
5 adversaries might be targeting the universities, so certainly
6 broader than just research.

7 **DR. LEAH WEST:** Thank you.

8 Mr. Jean.

9 **MR. DANIEL JEAN:** Maybe I can talk about
10 Australia, but start from the big picture to go to where they
11 are now.

12 In 2017, Prime Minister Turnbull basically
13 realize that Australia were up to their elbows into Chinese
14 foreign interference. And the move that he did, which was a
15 very interesting move, is he basically went and hired as a
16 special advisor, John Garnaut, who was journalist, lawyer by
17 training, who was covering China, sinologist. And he brought
18 him in, gave him all the security clearance and he paired him
19 with the Director of ASIO, who is the CSIS equivalent. And
20 he was basically given the task to internally look at all the
21 stones of foreign interference in Australia. At that time
22 they were focusing on some politicians, political donations,
23 that's the thing that you saw in the media, 2017.

24 When John Garnaut started to work with Asia
25 on all of those things, this is when he started to realize,
26 oh my God, our universities, particularly the Tier 2, the
27 ones who are struggling more for money. Students in
28 sensitive programs, this is when they started to see the

1 issue of diaspora intimidation and monitoring and all that.

2 So the first wave of measures were to deal
3 with their biggest issues. So they dealt a lot with, you
4 know, political donations, foreign -- they reinforce their --
5 the equivalent of what is -- over there it's one function,
6 the Election Director General and the Commissioner for
7 Elections; they reinforce that. They took a lot of measures.

8 John Garnaut actually, once this report was
9 done -- because what happened after that is the Cabinet look
10 at the threat assessment, they went with this and they
11 adopted all these measures, they started to come publicly.
12 At some point there's a Chinese affiliation that came to
13 this. John Garnaut, by the time that he was leaving was
14 actually hired by the universities to do their reviews
15 because of some of the things that had been identified.

16 So I'm just saying there that you've got to
17 understand the context of Australia, this came -- like, in
18 this Inquiry, we find intimidation of the diaspora is a big
19 issue, much bigger issue than what the common people know.
20 For the experts, not a surprise but the common people in
21 Canada.

22 But in the assessment in Australia this was
23 not the biggest issue at the time. They had much bigger
24 things. But through this they discovered that, and it became
25 in their second wave. Like, for example, they have their
26 first trials right now, they've been successful in the
27 Foreign Agents Registry, which was also created in 2017. So
28 my advice on this is you've got to make sure that what you're

1 creating is the right remedy for the -- right cure for the
2 illness that you have.

3 What I'm worried about when I hear the
4 conversation here is, yes, culture takes a long time, and
5 yes, you can take some short-term measures like what you're
6 proposing, Dick, but if it's only driven with a whip, it's
7 not something that they build and make it part of their DNA
8 that they're going to engage regularly, proactively, they're
9 going to be more sensitive to what the diasporas are, that's
10 going to be a problem. In the same way communicating to the
11 public you need to find a way to communicate that the
12 ordinary citizen understand why they should care.

13 You know, I see all the experts who say, "We
14 want a threat assessment, we want this"; I'm not saying it's
15 not necessary, but that's not what the ordinary citizen is
16 going to read.

17 So there is a way to come up with some ways
18 to get the citizen interested in to why they should care. Is
19 that -- you said three minutes, video-type approach where you
20 get to a case for them to understand why it is a concern that
21 they should care. Using credible third parties is very
22 important for all communication. But I'll leave it there.

23 **DR. LEAH WEST:** So this goes to my -- the
24 next kind of theme was that talk about culture change within
25 the organization. So not just making sure Canadians
26 understand the threat better, but that the organizations
27 understand the threat environment better so that they can do
28 their jobs, but then that level of culture change down on the

1 ground and engagement. And I guess I'm wondering what
2 advice, Ms. Gill, you would have for people thinking about
3 that kind of engagement that people on this panel all seem to
4 agree is necessary.

5 **MS. LEX GILL:** Yeah. It's interesting, I've
6 been thinking a lot about this since Mr. Jean's comment
7 regarding having sort of boots on the ground and going back
8 to tactics that might have been more commonplace in the past
9 around door-knocking, getting directly in touch, face to
10 face, with communities.

11 I mean, I have some real concerns about those
12 practices. I think Professor Carvin did a really great job
13 sort of articulating some of those concerns.

14 The reality is, you know, the trust in these
15 agencies is extremely low among civil society groups, among
16 diaspora groups, among human rights defenders, and that's not
17 for no reason. That's because, unfortunately, there have
18 been situations of abuse, of overreach, of surveillance of
19 Indigenous and environmental groups, of human rights and
20 anti-war groups, and the long shadow of the post-9/11 era.

21 And I think that it's important to understand
22 that some of those tactics are still taking place in ways
23 that are inappropriate, the sort of door-knocking and stuff
24 like that. And I think that we really need to have a totally
25 different perspective on how to build these relationships and
26 rebuild these relationships, you know.

27 And I think that sometimes when I hear people
28 -- and I say this with a lot of respect, when I hear people

1 sometimes from the intelligence community talk about the sort
2 of -- the frustrations around these tactics as a sort of
3 like, "Oh, that's a post-9/11 thing," like almost like people
4 need to get over it, we need to move -- this is not ancient
5 history in these communities. There are -- you know, and I
6 don't want to speak on -- you know, on behalf of Arab,
7 Islamic, and Sikh people, but what we hear from those groups
8 is the issues continue. And look, I mean, today also those
9 issues are also informing how those communities are
10 experiencing, like, government action around Palestine, which
11 I think is enormously complex and -- you know, I'll give a
12 very specific example. There was an entity recently added to
13 the Terrorist Entities List, okay? And without taking any
14 position on whether that entity should be on that list or
15 not, what I can say is that there has been a tremendous
16 failure of communication around that listing to the extent
17 that, you know, organizations that are organizing, like,
18 Shabot dinners for peace, all of a sudden think that, you
19 know, they might be treated as terrorists by their own
20 government.

21 And so the sort of chilling effect of these
22 kinds of decisions when they're not properly communicated,
23 when there isn't effective, meaningful, transparent
24 relationships with communities that are affected by the work
25 of our intelligence agencies, there's really serious
26 consequences for that.

27 And so in a context where the trust is very,
28 very low, the best practices look like dealing with

1 established leadership of these groups, of groups in these
2 communities, in transparent, open ways. And not showing up
3 at the mosque to talk to the person who's sitting next to you
4 in line, and not hanging out on campus at the vegan soup
5 kitchen or whatever to see what you might learn, because the
6 reality is those kinds of tactics, no matter how well-
7 intentioned, are going to create paranoia and mistrust and
8 anxiety that can be almost as intense and harmful as the
9 paranoia and mistrust and anxiety being created by the
10 foreign interference, so...

11 **DR. LEAH WEST:** Mr. Fadden, then Mr. Jean,
12 then Mr. Jones. So if you can keep your interjections brief.

13 **MR. RICHARD FADDEN:** I guess I'd just like to
14 present somewhat of a different side of the story that Ms.
15 Gill was just articulated.

16 There are occasions when knocking on a
17 person's door, when the person does not know you're coming,
18 could prevent a loss of life. There are occasions when it's
19 absolutely necessary, and I hope you're not excluding that in
20 every single case. But it seems to me, though, that the only
21 way that we're going to change -- we're talking about
22 bureaucracies here, we're talking about hundreds and
23 thousands of people.

24 So I think culture change is necessary. I've
25 tried to effect it in every job I've had, but if you're going
26 to change how CSIS interacts with members of the diaspora
27 community, the Director of CSIS is going to have to issue a
28 series of broad instructions about the range of tactics they

1 can use, when they can use them, and why. That will have
2 more of an impact than all of us, including myself, going on
3 and on in front of the Commissioner talking about cultural
4 change. We're dealing with bureaucracies. That's not the
5 same as a small law firm where you have 10 people or, you
6 know, an engineering firm, you have five people and you want
7 to change things. At some point you have to take whatever
8 the heck you're talking about and reduce it to standing
9 operating procedures, and I think in the end, that has to
10 come from Ministers telling the agency and the departmental
11 heads they have to do it.

12 I go back -- I mean, I agree with what Daniel
13 said. It's not ideal. I think cultural change from the
14 bottom is wonderful, but it is so slow, we need to find
15 alternatives to move it a little bit in the direction of
16 better practices, sooner rather than later.

17 **DR. LEAH WEST:** Mr. Jean?

18 **MR. DANIEL JEAN:** So to echo some of the
19 comments that Lex has made, I sit on the Transparency
20 Advisory Committee of the Deputy Minister of Public Safety
21 and we've issued a report on racialized and marginalized
22 communities, and when we were doing this report, we met with
23 a lot of the communities who are raising these concerns here,
24 and also we've met with the senior officials of the various
25 agencies.

26 For me, and by that time I was five years out
27 of government, so I feel as much as a civil person as I used
28 to for a long time to be a bureaucrat, and I just couldn't

1 believe the distrust. I basically felt that the way the
2 communities were describing what were my colleagues, I know
3 they're not that bad; right? And we've got to be careful not
4 to take the one thing that goes wrong and generalize that in
5 everything. It's true in every daily activity.

6 And then on the other hand, I could see that
7 there was efforts by the agencies to which they're engaged,
8 but they still saw that very much as engagement of we meet.
9 You know, it's punctual, it's not meaningful engagement, and
10 trying to change the culture of the organizations too. But
11 they're real efforts.

12 You know, Director Vigneault was very clear
13 to the Muslim community, "We need to protect you. You know,
14 look what's happened in Quebec. What's happened in London.
15 We want to work with you." Right?

16 So you need to close that gap, and you're
17 absolutely right, because we heard that as well, that they
18 still see that if they're coming to meet them, they're more
19 to get information than to give them information or to
20 respond to some of their grievances. So that part is very
21 much there.

22 These agencies, they do incredible
23 recruitment efforts to be representative of Canada. In fact,
24 CSE has a real challenge because in the computer science
25 thing, the labour market availability of people from visible
26 minorities is so high in Canada that CSE is very high, but it
27 keeps trying to jump. CSIS is doing some real efforts, but
28 sometimes people that would be very helpful may not wish to

1 come. I was sharing an anecdote of brilliant Sikh analyst
2 that worked with PCO wanted to go work for GAC. I said,
3 "Getting a job at GAC is like winning the lottery. Here are
4 all these organizations that have international --" and then
5 when I said, "CSIS, they could really use somebody like you
6 for what we're discussing today," and he looked at me, and,
7 "I could never do that."

8 We have to find ways to change this distrust,
9 because otherwise it's not going to happen.

10 **DR. LEAH WEST:** Mr. Jones, and then Ms. Gill.

11 **COMMISSIONER HOGUE:** I think, because I'm
12 looking at the clock, there's one question that I would like
13 you to address in connection with this one, because you're
14 focusing on the various communities, which is absolutely
15 useful, but I would like also to get your views as to whether
16 you think we also need to engage in, and to a certain extent,
17 educate the Canadian in general about what we are speaking
18 about? What is national security, what CSIS is doing, what
19 CSE is doing. So I'm asking the question. Anyone can
20 answer.

21 **DR. LEAH WEST:** Mr. Fadden?

22 **MR. RICHARD FADDEN:** I think absolutely. The
23 issue is not whether we should do it, it's how we do it. I
24 think it goes to the definition of national security.
25 Shantona and I were talking in the meeting room about the
26 definition of intelligence. Nobody understands what the
27 devil intelligence is, and the minute you say "intelligence",
28 everybody's blood pressure goes up, you know, by 50 percent.

1 So even something as simple as that, so the
2 question is who can do it effectively, and using what medium?

3 If you -- you will have gathered from my
4 earlier comments that I think that a lot of these issues, the
5 further you keep Ministers from this, the better off you are.
6 Not that they're not ultimately responsible politically, but
7 if you have, within the Public Service, for example, a
8 requirement that for all of the kind of communications,
9 Commissioner, that you're talking about, they would have to
10 be reviewed by Ministers, and depending upon the time of
11 year, the period in the electoral cycle, risk aversion would
12 prevail and we would go off on a tangent.

13 To pat myself on the back, I think my panel
14 of the great and good have given sufficient resources and a
15 mandate at some distance from government, and I mean a mixed
16 panel, I don't mean people from the security community, would
17 be better placed to start doing all this kind of
18 communications, using government resources if need be, but
19 the planning and the strategy being taken a little bit out of
20 government because it's the sort of thing that if you're a
21 Minister, there's no win. There's no way you can have this
22 communication without having somebody somewhere accuse you of
23 all sorts of nasty things. So I would say absolutely yes.
24 Who? Some distance from government.

25 And it's the sort of thing where you're going
26 to have to repeat it until you want to kill yourself almost,
27 because people do not register these things initially. It
28 would have to be an ongoing campaign modified over time.

1 It's just -- people just don't remember these things unless
2 it affects them personally. So it would have to be an
3 ongoing permanent effort, I would submit.

4 **DR. LEAH WEST:** Dr. Carvin, I just want to
5 add to that, on top of that, we've heard a bit about
6 different institutions or organizations that could be
7 proposed to do this. So we've heard about changing the role
8 for the Panel of Five. We've also heard about the Australian
9 model for Centre for Foreign Intelligence, National Security
10 Council, and, you know, there's two other things I want to
11 put on the table about organizations that we haven't talked
12 about that might be models.

13 One is, is there a need for a foreign
14 intelligence agency? How would that come into play here?
15 That is a question we have received.

16 And the other one is thinking to the Canada
17 Centre for the Prevention of Violent Extremism and its model
18 of funding and education and whether or not that might be
19 something useful in this space.

20 So Dr. Carvin?

21 **DR. STEPHANIE CARVIN:** I will address those
22 two points, but just coming off the question about who should
23 do education, I think I spent the first part of this panel
24 promoting my research, and now I'm going to ask for funding.

25 So we can also ---

26 **COMMISSIONER HOGUE:** I'm not the one who can
27 ---

28 **DR. STEPHANIE CARVIN:** Just if anyone is out

1 there. Government.

2 But the -- not just entirely self-serving,
3 but it's also about, you know, how do we better -- how do we
4 get Canadians to better understand this?

5 I mean, there are very few programs out there
6 at the secondary educational level that really deal with --
7 or sorry, second or third tertiary education that teach these
8 issues; right? I mean, we could start with, like, just basic
9 civics would be helpful I think generally in understanding
10 our democracy better, and strengthening our democracy goes a
11 long way just to do that. That's probably outside the scope
12 of the Commission, but, you know, better funding programs
13 that deal with security intelligence issues.

14 It's sometimes hard to get funding. I
15 understand, because sometimes the research bodies say, "Well
16 this should be funded by the government," then the government
17 doesn't really necessarily want to fund a bunch of -- I'm
18 tempted to use -- I'll just say academics, because we're
19 academics. And I get that too.

20 But I think even just creating better
21 education about these issues at, you know, the graduate
22 level, the undergraduate level, even perhaps having more
23 experience in high schools I think would -- or CEGEPs would
24 be helpful on that.

25 So I think, like, just creating, again, more
26 -- is there a need for courses on foreign interference? Is
27 there a need for courses on the diaspora experience? Right?
28 Better understanding what these -- who these diaspora are and

1 what their experiences are. I think it doesn't just have to
2 be from a security lens. It could be from, like I said,
3 anthropological, social work, all those other kinds of
4 things.

5 Regarding a foreign intelligence agency, wow.
6 I mean, like, if we're playing fantasy national security,
7 sure, it would be great to have a foreign intelligence
8 agency.

9 One of the things you hear in talking to our
10 allies is, you know, you often hear kind of talk about how
11 bad Canada is at national security and how our institutions
12 are a joke and we're going to be kicked out of the Five Eyes.
13 And I want to stress how much that's not true, that actually
14 Canada is respected in the Five Eyes.

15 The problem isn't that we're not respected,
16 the problem is they want more of us; right? They want us to
17 do more. They -- you know, this is often what you hear from
18 our Five Eyes partners.

19 So yeah, a foreign intelligence agency would
20 be great. Is it the best place to put limited resources now?
21 I don't know.

22 Where would that intelligence agency go?
23 Would it be part of GAC? Would it -- you know, people think
24 you can just kind of tack it on to CSIS, but it would be
25 operating under an entirely different legal regime and I
26 think it would put real strains on that organization.

27 It's a really difficult, perplexing
28 challenge, and as we are confronting the threat of foreign

1 interference -- yeah, I think -- the benefit of a foreign
2 intelligence agency would be that you would -- we're so
3 heavily reliant on other countries that when we get their
4 intelligence, we're getting it from their perspective. It
5 reflects their interests, it reflects their priorities.

6 If we were thinking about how foreign
7 interference would help us, yes, it would give us a better
8 understanding, I think, of what the priorities of those
9 governments engaging in foreign interference in Canada
10 actually is, but I'm just not sure it's the best use of our
11 money at this time as much as I think it would make our
12 allies happy and possibly add a little bit of understanding.

13 But I think the priority needs to be just
14 fixing the mess we're in now, and I'm not sure the foreign
15 intelligence agency would do that.

16 I'm a fan of the Canada-centre model. The
17 Canada-centre model is where it's kind of foreign -- like
18 they say it's at the national level. It provides funding at
19 provincial level, provincial level -- I think there's five
20 institutions that it presently provides money to. There's
21 Shift B.C., there's one in Alberta. I think the Organization
22 for the Prevention of Violence. There's the Yorktown Centre
23 in Toronto. And then there's two in Quebec.

24 It's good, right. I mean, the issue with
25 those organizations is how well they have done in terms of --
26 you know, they're more in demand. Like they actually need --
27 they need more resources, not less.

28 They've actually done well, and communities

1 have learned that they can go to those organizations because
2 they're not the police, right, even though sometimes they're
3 referred to -- in cases they're referred to by police, and
4 they get the help from a public health perspective, not a
5 security perspective. And I think that's really important.

6 So there's lessons to be learned there.

7 But that being said, foreign interference is
8 very, very different from radicalization, right. And you
9 know, with radicalization you're trying to get people help
10 and interventions and counselling and things like this. So I
11 don't know what it would do other than kind of be a
12 repository for information.

13 It might be a better model for community
14 engagements because it's not CSIS and people might feel safer
15 going to those organizations knowing they're talking to the
16 government. Maybe you could triage it.

17 But we'd have to put some thought into it. I
18 don't think it's an automatic cut-and-paste model you could
19 just kind of throw into the provinces.

20 **DR. LEAH WEST:** Dr. Robson-Morrow and then
21 Mr. Jean.

22 **DR. MARIA ROBSON-MORROW:** Thank you very
23 much.

24 This will be a brief point going back to the
25 discussion of building and understanding of the intelligence
26 agencies, the idea that we on the panel may understand the
27 differences between CSIS, CSE, what they do, what
28 intelligence is. This is not something we should take for

1 granted.

2 On that point, there is discussion the Five
3 Eyes have about proactive disclosure of intelligence and the
4 idea of disclosing successes, not just allowing the narrative
5 to be around failures or shortcomings. So I did want to make
6 sure we touched on that, this idea of encouraging more of a
7 culture of highlighting what intelligence can actually do in
8 a way that does touch communities, touch Canadian democratic
9 processes, protecting the public because intelligence risks
10 being the goalie. No one remembers the shots that don't go
11 in, remember the failures. We don't necessarily remember or
12 know about or be able to know about the successes.

13 And going back to Ms. Fadden's comment about
14 us being risk averse, we talk about the culture of secrecy.
15 CSIS was born out of the perceived overstepping out of the
16 MacDonald Commission, was born deliberately with safeguards
17 and constraints on it, so I think there's value in thinking
18 about ways to disclose intelligence.

19 Just in the past few years, we saw in the
20 lead-up to the Russian invasion of Ukraine the Five Eyes
21 proactively disclosing intelligence, revealing the game play
22 in a way that this was in the news, particularly when Ukraine
23 was invaded. It was all over the news, and so there was an
24 understanding of what intelligence agencies have been doing
25 behind the scenes to try to effect an outcome that we all
26 understood to some extent.

27 So just thinking about -- I'd suggest that we
28 should think about -- the intelligence community should be

1 thinking about ways to proactively disclose this type of
2 thing.

3 We can remember the Toronto 18 as a rare case
4 where we actually understand that intelligence agencies
5 contributed to a positive public security outcome, so
6 thinking about more ways to build credibility and build an
7 understanding of what intelligence is and what the agencies
8 do.

9 Thank you.

10 **DR. LEAH WEST:** Mr. Jean?

11 **MR. DANIEL JEAN:** Reacting to a few of these
12 points.

13 First of all, Panel of Five, agree on
14 independence, but we've got to be careful to see, first of
15 all, whether there's existing mechanisms in place,
16 independent mechanisms in place like Director of Elections,
17 Commissioner of Elections that can take some responsibility,
18 and then what's left.

19 I agree with the objective on communication.
20 I have my doubts that if you were to create the organization
21 they would communicate differently than our review mechanisms
22 that exist do, which is the same, issuance of reports that
23 are not read.

24 I applaud their work. I read it. But to the
25 citizens, they don't read it.

26 So I like the -- what -- your question about
27 the radicalization council. I've been exposed to it. What
28 is interesting is that model is because you go try to

1 leverage people closer to the citizens or to the community,
2 so you really leverage these third parties which I was
3 referring before.

4 I said before, be very careful. There's a
5 bit of an habit of where we have a problem, let's create a
6 structure, right. And most of the time, it takes a lot more
7 than structure to create problems.

8 We're also in an environment where money is
9 going to be rare, I think, here, given our fiscal situation.

10 And there's also -- the other thing that you
11 hear very often is centralization, everything in PCO. You
12 know, PCO would become the department of all departments.
13 But the resources are in organizations.

14 After 9/11, it was probably a normal reflex,
15 we centralized a lot of things in PCO and then we suddenly
16 found if you want things to be happening, PCO has to play its
17 role, but the energy, the efforts, the talent is in the
18 department. You need to responsilize (*sic*) them in doing
19 that.

20 The foreign intelligence Five Eyes, I love
21 what you said. I travel -- you think the NSA doesn't stay in
22 place too long in Canada? I had four U.S. NSAs during my two
23 years' term as NSA in Canada.

24 I met a lot of the NSAs around the world,
25 these agencies, and what I hear is what Stephanie described,
26 which is to say, Five Eyes is a work-sharing mechanism.
27 Their expectation is not that we're going to produce the same
28 volume or the same thing they produce. A work-sharing

1 mechanism is that you bring the expertise in a complementary
2 way and what they love is we bring added value. As long as
3 we bring added value, we'll be welcome.

4 My concern with the foreign intelligence
5 agency has always been the same. We are very good, I said
6 that earlier, at the beginning. We create structures, we
7 don't resource them, and we wonder why they don't work.

8 So I would much rather have a very strong
9 national security apparatus that functions well, that does
10 well, that provides its added value to our allies and
11 partners like the Five Eyes than rather to create another
12 structure but not equip them to be able to do what they need
13 to do.

14 **DR. LEAH WEST:** Ms Gill.

15 **MS. LEX GILL:** Yeah, it might be a minute
16 since this was like really relevant, but I do just want to
17 offer like a little bit of a synthesis of some of the themes
18 that are coming out here in the sense that I think that
19 sometimes there is this tension or conflict that's being
20 presented between being transparent and being effective or
21 respecting human rights and being effective as an
22 intelligence agency, and I think that, in fact, a lot of the
23 comments are really circling around this idea that one can
24 feed the other in the sense that, if there is proactive
25 disclosure, if there are strong relationships that are built,
26 if there is really a robust culture of justification, of
27 transparency, of openness, of explaining what it is that
28 these agencies do to the public within government, then that,

1 over time, can build a foundation of trust and legitimacy,
2 and that becomes self-reinforcing.

3 And so I think that it's important for us to
4 step away from a paradigm where these things are necessarily
5 in conflict and, instead, look to ways in which they can be
6 more reinforcing.

7 So I just think it's -- it would be helpful
8 in the Commission's work to think about that not as a zero-
9 sum conflict.

10 **DR. LEAH WEST:** Going back to the
11 Commissioner's question about education, one of the questions
12 from a party was about the idea of doing a national threat
13 assessment before Parliament, or something to that effect,
14 where there is an annual kind of airing of threats to the
15 Canadian public.

16 Does anyone have any thoughts about the
17 success of that kind of mechanism?

18 **MR. RICHARD FADDEN:** To be honest, it's
19 something that's been advocated for the last 15 years, not
20 exclusively with respect to foreign interference, but more
21 broadly in the national security area.

22 We've never succeeded in doing it. I mean,
23 CSIS produces something, Defence Department produces
24 something, FINTRAC produces something, and you know,
25 sometimes the assessment unit at PCO sort of pulls things
26 together for internal use, but Ministers have very strongly
27 resisted doing a global threat assessment, certainly in my
28 time, despite the fact that all of our allies, to one degree

1 or other, do it. I personally believe that we're barking up
2 the wrong tree if we're suggesting this.

3 Also, because anything that has to be tabled
4 in Parliament becomes so milquetoast by the time it's gone
5 through the various, you know, checks and balances for
6 partisan purposes. If it's done, it's not going to harm
7 anybody. And it may well help. But if we put all of our
8 money in that particular approach, I don't think it will have
9 the practical effect.

10 For us in the bubble? Absolutely. For a few
11 of you in universities? Absolutely. A few journalists. I
12 was in Toronto recently on something totally unrelated to
13 this, and I started talking about some of this, and all I
14 got, from very intelligent, well-educated people, utterly
15 blank face. My son lives in Vancouver, exactly the same.

16 So, a parliamentary report on threat
17 assessments, I think it's a good idea in and of itself, but
18 it's not going to, I think, solve the problem that we're
19 talking about.

20 I think -- I'm old enough to remember
21 Information Canada. I don't know if any of you do? It was a
22 funny agency that I think the first Trudeau Government
23 created to try and get governmental information out. And I
24 think, on balance, because that's all they did, and they had
25 a fair bit of resources, they had some measure of success.
26 It was outside of any particular department and agency, but I
27 think -- at least in the short to medium term, maybe that's
28 somewhere to go, or add that on to another department or

1 agency.

2 But it's going to take, I would argue, a
3 standalone effort, whether it's within an agency or in a new
4 agency. And I come back to my point, I apologize, it has to
5 be at some arm's lengths to Ministers or everything that's
6 produced will be so risk averse and so diluted that nobody
7 will read it.

8 **DR. LEAH WEST:** Mr. Jean?

9 **MR. DANIEL JEAN:** If you want a more
10 effective communication with the citizens, you have to be
11 able to show them why they should care. And we've had a very
12 interesting experience like when we did the Graduate School
13 of Ottawa U Report on National Security about two years ago,
14 Dick was on it as well, co-authored by Thomas Juneau. When
15 we released our report, the biggest coverage, all newspapers,
16 some television, some continue to quote it in Quebec.

17 And as a Quebecker, I personally think that
18 one of the reasons why Quebeckers care more and their
19 journalists care more about this report than in some of the
20 rest of Canada, because Quebec is not -- Madame la
21 Commissaire, vous allez être d'accord avec moi, c'est pas la
22 province qui est la plus sensible à la sécurité nationale du
23 Canada, mais pourquoi qu'ils s'intéressaient à ça en
24 particulier? C'est la province qui est la plus dépendante
25 des exportations vers l'étranger, et en particulier vers les
26 États-Unis. Il y a pas de *better US watch in Canada* qu'au
27 Québec. Il y a des chroniqueurs dans tous les journaux,
28 toutes les TVs, parce que ça... *they care*, parce que ça... c'est

1 leurs emplois, c'est leur... qui dépendent de ça.

2 Donc, de là, ce que j'essaie de dire, c'est
3 qu'il faut trouver pourquoi les Canadiens devraient se
4 préoccuper de ça. Pis il faut être capable de faire ça dans
5 un langage simple pis dans des images pis en utilisant des
6 tierces parties qui vont ramener. Parce que sinon, ça va
7 être épée dans une marre d'eau.

8 **DR. LEAH WEST:** Commissioner, did you have a
9 question that you'd like to ask? If not, I have many, but
10 I'll turn it to you.

11 **COMMISSIONER HOGUE:** No, go ahead, and I'll
12 ask my question -- I find a way of asking my question.

13 **DR. LEAH WEST:** There's been a lot of
14 discussion over the past few weeks about who read what, when,
15 how, whether or not it was sufficiently communicated, whether
16 or not the analysis was reflective of the issue, people
17 digesting the intelligence, et cetera. So, the nitty-gritty
18 of intelligence analysis and digestion and sharing of
19 intelligence analysis. We did hear a bit about it from
20 Dr. Carvin and Daniel Jean, but I was just wondering if
21 anyone else wanted to speak to that issue in particular,
22 about augmenting Canadian intelligence analysis capacity,
23 centralizing it, et cetera.

24 Anyone? Mr. Fadden.

25 **MR. RICHARD FADDEN:** I'm going to, to some
26 degree, reverse what I've been saying about Ministers. I
27 worked off and on in national security since Mr. Chrétien and
28 9/11. And the extent to which the community is a resource,

1 the extent to which the community is listened to, the extent
2 to which they can have an impact, is almost exclusively
3 dependent upon the views of the Prime Minister of the day.

4 I would argue, with great respect, the
5 current Prime Minister is not particularly interested in
6 national security, and that permeates the system. I'm not
7 saying he's disinterested, but he's not particularly
8 interested.

9 Somebody was saying a little while earlier
10 about, you know, getting information up and making sure it
11 goes. I was in PCO during the end of Mr. Harper's time, and
12 we were still involved in Afghanistan, and let me assure you
13 that if the community had anything on Afghanistan, he got it.

14 So, I cannot overstress the importance of the
15 *tournure d'esprit* of the Prime Minister, because he does have
16 a special role in national security. And because political
17 power is so centralized in Canada, even if you have a Public
18 Safety Minister who's the most enthusiastic man or woman on
19 the planet, if the PM ain't interested, you can create new
20 assessment regimes, you can create new -- I think Daniel and
21 I disagree a little bit, I think the National Security
22 Council is smoke and mirrors. If the Prime Minister is
23 interested in national security, you can have the effective
24 conversation around a coffee urn. If he is not interested,
25 you can create all sorts of institutions, which may help, but
26 won't solve the problem.

27 So, I think in the final analysis, you know,
28 more assessment units, better communications, all fixable up

1 to a point beneath the level of Ministers. But if the Prime
2 Minister or the government of the day, unlike the United
3 States, unlike the United Kingdom, unlike France, not
4 fundamentally interested, it's sort of like pushing
5 spaghetti, if you'll forgive my use of the analogy. They are
6 really critical in this.

7 And the counter to this is that when we have
8 a real crisis in Canada, it's amazing how we galvanize
9 ourselves. But people have not come to the conclusion yet
10 that FI is a real crisis. 9/11 was a real crisis. SARS, to
11 your point, was a real crisis. And I think, I hope,
12 Commissioner, you can factor some of this in your
13 recommendations because if the PM of the day, whether it's
14 Mr. Trudeau or Mr. Poilievre, are fundamentally disinterested
15 and we can't convince them that it's worth doing something,
16 yes, some change will take place, but, boy, it's going to be
17 an uphill battle.

18 **MR. RICHARD FADDEN:** Mr. Jones.

19 **MR. ALAN JONES:** Thank you. If I could
20 follow on to what Dick and Danielle have said, I think
21 there's multiple layers to how you respond to foreign
22 interference or any other national security inquiry.
23 Absolutely, if a Prime Minister is marginally interested or
24 not interested, it has an effect. Or if a Prime Minister is
25 really interested, it has an effect.

26 But in -- and when I raised the issue of --
27 and I, you know, colloquially use the term National Security
28 Council, but some more permanent structure than we have, one

1 of the purposes of permanent structures is to even out those
2 waves, is so that the government, the operational arm of the
3 government, always remains capable of doing something,
4 regardless of whether the Prime Minister is super interested
5 or even marginally interested. And there is work that has to
6 be done every day because there is legislation.

7 I'll give a very quick example of the
8 question of variation of the Prime Minister as being
9 interested or not interested. I'm not going to say which
10 Prime Minister it is or which National Security Advisor it
11 was, but I was at PCO, my phone rang, I was in my car. The
12 National Security Advisor said to me, "I'm with the Prime
13 Minister. The Prime Minister is reading something on the
14 front page of *The Globe and Mail*. He wants to know if
15 someone is dealing with this, or does he have to give the
16 order for somebody to deal with it?" I said, "You can
17 reassure him, he does not have to give an order. There are
18 officials in government who are dealing with this already.
19 It's what they do every day."

20 So, the more -- the more effective that the -
21 - those daily operations are, the better off we will be in
22 terms of the quality information that is eventually provided
23 to a Prime Minister, whether they want it or not sometimes.

24 And when we talk about the quality of
25 intelligence, as I've said before, the quality of
26 intelligence reports going up often depends on the quality of
27 the requirements and requests coming down.

28 When we say, "What is it that they're looking

1 for?" And if you don't know exactly what they're looking --
2 what your seniors are looking for, you tend to write very
3 broad documents trying to, at some point, hit the mark
4 somewhere along the line to see whether they're in or not.

5 The more sophisticated they are -- and the
6 Prime Minister job and senior jobs are enormously busy.
7 There's an awful lot going on. And so, you're not going to
8 get much of their time, because they're trying to deal with a
9 lot of things. But if they're supported by a more, I don't
10 want to say professional, because people work extremely hard
11 in these areas, but a more permanent structure which can
12 manage some of these requirements as to what intelligence is
13 expected out of government.

14 And Dick has raised this earlier about
15 organizations getting orders and being told, "Do this." And
16 very broad intelligence priorities become very broad
17 generalized annual work plans. Politicians, elected
18 officials, and often senior government officials, are caught
19 in somewhat of a contradictory position where they want to
20 know more, but they're afraid to give specific direction to
21 an intelligence service or police agency to do specific
22 things. They don't want to be perceived as directing that an
23 investigation be conducted against an individual or a group,
24 because that would make it a politically motivated
25 investigation.

26 But at the same time, they know that they're
27 supposed to know more about this issue and need to do
28 something about it at a policy level, and they would like to

1 have more information than they did.

2 ITAC was created as a result of a Prime
3 Minister at the time, Paul Martin I think, who said, "I'm
4 tired of getting five or six different threat assessments on
5 the same issue which don't say -- are not a singular
6 authoritative voice on the issue." And of course, those were
7 very tense times, but that happens every day.

8 So there is a requirement to have better
9 quality intelligence, but also better-quality requirements,
10 and all of that requires, as Dick said, taking this more
11 seriously at multiple levels.

12 **DR. LEAH WEST:** I wonder if Professor Carvin
13 or Dr. Morrow, if you could speak to this idea of a more
14 empowered NSIA and how that might facilitate some of that?

15 **DR. STEPHANIE CARVIN:** Thank you. Sorry,
16 yeah, so it's Professor Carvin, just for the transcript.
17 Just to be sure.

18 So yes, in answering that question, I just
19 also want to touch on what was just said. The research I did
20 with Professor Juneau on our book really confirms what Mr.
21 Fadden said in terms, when we interviewed them, they read
22 intelligence because they thought the Prime Minister was
23 reading the intelligence; right? There is this real trickle-
24 down effect in terms of the community. You read what your
25 boss is reading. And so, you know, if your boss is
26 interested in sunny ways and national security is dark and
27 stormy, there's a tension there in terms of that, and I don't
28 think we see this in other countries where I think even if,

1 you know, Donald Trump was said to be not interested in
2 intelligence, there was a lot of people around him, and a lot
3 of people in the U.S. community that still were reading those
4 products. I'm not sure that's true in the Canadian case.

5 **COMMISSIONER HOGUE:** Do you have any idea why
6 it's different?

7 **DR. STEPHANIE CARVIN:** Our community is much
8 smaller. Our political -- our politicians don't necessarily
9 have clearance. I think Cabinet generally -- until -- this
10 is where I'm really curious to see if the Committee plays a
11 role in educating more Cabinet Ministers about intelligence
12 and how it's used and how it's made and what those issues
13 are. This, I think, is going to be a real test, to see what
14 the pull of the -- we can push -- as, you know, Mr. Fadden
15 said, it's -- you can push spaghetti all you want, but we
16 need them to pull the noodles. If they're going -- this is a
17 terrible analogy, but, you know, we need our Cabinet
18 Ministers to do more pulling of products, and that's the key
19 test. And I think that's going to be one of the key metrics
20 of the National Security Council. Do we see more departments
21 and agencies pulling products that are related to their
22 mandate?

23 And I would agree that -- and then hopefully
24 that would trickle down into the intelligence requirements
25 process.

26 One of the key problems, and the NSICOP did a
27 brilliant review of the intelligence requirements process, I
28 think back in 2017/2018, and they showed that one of the key

1 challenges there is that with the intelligence requirements,
2 everything was, like, a number one priority. Like, if
3 everything is a priority, nothing is a priority. So
4 encouraging, you know, better understanding of how the
5 community works would, I think, help that as well. And that
6 is, I think, another area where the NSIA would come in in
7 helping to perhaps provide more guidance on those processes
8 around the intelligence requirements.

9 The other area where I think a more empowered
10 NSIA could play a better role in this is being a better
11 facilitator of communications.

12 One of the things that has really struck me
13 about what we've learned about foreign interference is how
14 CSIS and other intelligence agencies have been trying to
15 communicate this to the government. And you know, CSIS was
16 basically portraying foreign interference as this ever-
17 looming -- you know, we've all talked about this. It's this
18 giant threat requires an all-of-government response, all-of-
19 society response. It's in our politics. It's in our
20 schools. It's in our universities. It's everywhere, right,
21 the way we've been talking about it.

22 And I think the analogy I would use is CSIS
23 was kind of talking about foreign interference like it was
24 talking about climate change; right? It's everywhere. It's
25 affecting all aspects of our lives. It's very complex.
26 Requires a whole-of-society response. And the Prime
27 Minister's Office was looking for a tornado warning. They
28 were looking for actionable intelligence pieces from those

1 assessments, and that's not really what CSIS is good at.
2 They don't really do opportunity analysis. They don't do
3 options analysis. They don't really provide the guidance
4 then. They can present the threat, not necessarily what to
5 do about it. And this is where I think an empowered NSIA
6 with a secretariat, with -- better able to coordinate the
7 community as a whole, could provide a much better job of
8 taking the climate change and tweaking it and creating those
9 maybe not tornado warnings per se, but taking those very
10 specific things that could be done, and then presenting that
11 to government, because that I think is really the missing
12 piece.

13 Like, you can present -- you know, like, you
14 can be in the doom and gloom, you be in the dark and stormy,
15 but unless you're providing some kind of very specific
16 actionable things that the government can do, it's not going
17 to work. And I would like to think that that is where an
18 enhanced NSIA, whether its mandate is spelled out in law, or
19 perhaps a better just understanding -- I think I saw in one
20 of the documents someone referred to a mandate letter, could
21 actually work.

22 **DR. LEAH WEST:** Any of the former NSIAs want
23 to jump in on that?

24 **MR. DANIEL JEAN:** I spoke openly, I thought,
25 on that at the beginning of the thing. There was a tornado
26 that they saw. It was the U.S. election. That became --
27 it's not -- I prefer the word "shiny object". Politicians
28 are attracted to shiny objects.

1 So we warned them about what happened in
2 Montreal with what and how the Russians could mount this
3 information campaign. There's a so what for Canada. It
4 happened in Canada, there was some Canadians, but so what;
5 right?

6 Three months later, there's the U.S. election
7 interference. Interest? Tornado? Boom. Spike.

8 Okay. The challenge is there to say, "Yeah,
9 but we don't think --" and how many people have testified,
10 former NSIAs and things, we don't think elections is the
11 biggest threat in Canada. And so far your Phase 1 shows it's
12 probably not -- there's some local risks, political parties,
13 something that has come up.

14 So we work very hard in saying, "Yes, we need
15 to strengthen our elections, the cyber role, the CSE, the
16 creation of the Panel of Five," all of that is important, but
17 we think foreign interference is deeper than that. Like, so
18 that's how far I'm going to go into an open panel, but I
19 think the difference is not that the mandate wasn't there,
20 that the -- there was no action about that, I would agree
21 with you. Like, that's what CSIS was doing. At that time,
22 there was nothing that was most of it actionable.

23 But the issue is there was nothing shiny, and
24 then the U.S. election was shiny, and said, "Well, that must
25 be big." So they -- and we were successful in saying, "No,
26 it's not just going to be cyber. The briefing with political
27 parties should be, you know, by CSIS as well and the rest of
28 the threats."

1 But it goes back -- that's why in my remarks,
2 I say you've got to find a way to make sure that the
3 political class is engaged, it's not just attracted by the
4 shiny objects. But I've seen politics long enough to know
5 that they're not going to be attracted by things if they
6 don't feel their citizens who vote are attracted by things.

7 **DR. LEAH WEST:** I do want to -- but this ties
8 into something that you talked about before, and one of the
9 things that came up in the NSIRA report that looked at this
10 policy decision-making flow was that the policies and
11 processes developed in the wake of the 2016 election, so SITE
12 and the CEIPP, was meant to address foreign interference like
13 what we saw in the 2016 election, and it necessarily hasn't
14 adopted to foreign interference as it actually plays out in
15 Canada. And I'm wondering if you might want to speak to that
16 in response to Daniel Jean's point, but also thinking about
17 your recommendations for the Panel of Five?

18 **MR. RICHARD FADDEN:** Sure. I mean, you
19 asked, Commissioner, a few minutes ago, in response to what
20 Stephanie was saying about why Ministers aren't interested,
21 and Daniel gave an answer I don't disagree with, but in my
22 experience, they do not feel threatened. Unless they feel
23 threatened, they don't act.

24 And fundamentally, that reflects the way
25 Canadians feel. We have three oceans and the United States'
26 border. We don't feel threatened in the same way as the
27 Americans, as the Brits, and even as the Australians. And
28 yes, they will be attracted to shiny objects. I think you're

1 right. But what really captures their attention is a threat,
2 and there I go to agreeing with a number of my colleagues
3 here saying part of the responsibility for that is how that
4 threat is described and brought to their attention. And I
5 think Al is right when he says in the absence of clear
6 direction, the default is generalization. And my experience
7 anyway, Prime Ministers, in particular but ministers,
8 generally, hate generalizations. They don't mind
9 generalizations when they're talking to the public, but when
10 they're being told about things, they want the specifics.
11 And there are instances where that's provided, there's no
12 doubt about it, but broadly speaking, most of the threat
13 assessments that have been produced certainly when I was
14 there, a couple that I've seen since then, they're too
15 general. And, you know, they've got better things to do, and
16 they just don't pay attention. And I would argue forcefully
17 that it's the issue of threats. And Daniel is right when he
18 says if the Canadian public does not feel threatened,
19 Ministers are not going to focus. And there, there is a
20 responsibility for the community to try and articulate these
21 threats, which is why initially, Commissioner, I suggested
22 that it would be helpful to you and your recommendations if
23 you can come down clearly and say there's a clear and present
24 danger. Pay attention to what I'm going to say in my
25 subsequent 600 pages or 30 pages. I don't know how long your
26 report will be.

27 **COMMISSIONER HOGUE:** Probably more than 30.

28 **MR. RICHARD FADDEN:** But less than 600? You

1 never know?

2 **COMMISSIONER HOGUE:** I don't know.

3 **MR. RICHARD FADDEN:** I've now forgotten what
4 you asked me to comment on. I'm sorry.

5 **DR. LEAH WEST:** So I will tell you, but I
6 guess I want to interject there and say, but Canadians do
7 feel threatened. They're probably just the ones that are the
8 most disconnected from the state, and I think how we bridge
9 that gap is an important thing that we've also brought up is
10 there are large subsets of Canadian population who do feel
11 threatened, but they're not the ones communicating with their
12 politicians, and how do we bridge -- fix that is also an
13 element of it. The other point I was asking you about was
14 the -- you know, the policy was designed to deal with one
15 particular threat to democratic institutions, which was what
16 we saw in 2016 election, but that's not what we're seeing as
17 the major threat to Canadian democratic institutions. So is
18 there a way of adjusting the policy, or does it need to be
19 revisioned, or you think it's sufficient as it is, given what
20 we now know is where we see foreign interference in Canadian
21 democratic processes. So I'll let you answer ---

22 **MR. RICHARD FADDEN:** I'll just ---

23 **DR. LEAH WEST:** --- and then ---

24 **MR. RICHARD FADDEN:** --- I'll do it very
25 shortly, but I think, absolutely, it has to be changed. Our
26 understanding of what's happening with foreign interference
27 is entirely different than what it was five, six, seven,
28 eight years ago. And to suggest that those initial efforts,

1 which are all in good faith and had some positive impact
2 would apply today, given the changes in the world generally
3 and what's happening in Canada, we're dreaming in
4 technicolour. So I think somebody has to take a very deep
5 breath and look at these things again, both the policies and
6 whatever structures we decide to put into place.

7 So I think -- I, in fact, as a Canadian,
8 never mind somebody who's putzed around in this area, I
9 really worry how we're going to deal with the next federal
10 election. I mean, so far, the government has talked in
11 generalities about how it's going to deal with the issue.
12 With great respect to the Commissioner's report, it may be
13 too late for them to implement any number of your
14 recommendations, even if they were inclined to.

15 But I agree with you, what was put into place
16 for the two elections that the Commissioner is particularly
17 charged with looking at, totally inadequate for today.
18 Totally inadequate.

19 **DR. LEAH WEST:** M. Jean?

20 **MR. DANIEL JEAN:** So I'm going to -- you
21 asked on that, I agree with some of that, I agree with your
22 question that it was created because they foresee what --
23 given what happened in the U.S., it would be kind of a
24 national approach to interfere, we'd look at what happened in
25 France and Germany, a lot of conversations with these folks.
26 But despite that, when you look at your proceedings, I've
27 been watching very carefully, some of the local level things,
28 they came up in the Task Force. So it's not like they were

1 not picked up.

2 We go back to the threshold, and then we also
3 go back on the panel position. I think that it's really
4 difficult -- we don't need to repeat what -- very difficult
5 to ask people even though they're non-partisan, we're serving
6 the executives to be making these kinds of decisions. You've
7 had Jim Judd and then Morris Rosenberg would reviewed the two
8 elections, all the material that they've had. I look at
9 Morris Rosenberg, he raised a question is the threshold too
10 high. Now the danger, of course, is the reason why the
11 threshold is high, and it relates to what you've said
12 earlier. You're going to make sure that going public is not
13 going to make it worse than not doing things; right? You
14 don't want to interfere in the election either; right?

15 So I think that definitely the Panel of Five
16 needs to be reviewed. The Task Force itself that they go and
17 have an understanding that it's bigger than what it was
18 created for. Yes, but in practice I would argue they were
19 already -- their job certainly, despite the fact this is not
20 what was expected from what I've seen in both in the
21 Rosenberg report, the Judd reports and some of your
22 proceedings. I mean, what you've found is some local things;
23 right?

24 **DR. LEAH WEST:** Last moment, I'll turn it
25 over to the Commissioner.

26 **COMMISSIONER HOGUE:** No, except for saying
27 thank you to everyone. Honestly, I think we'll be able to go
28 on for hours and hours and maybe for days and days, but even

1 what we have been able to cover this morning was very, very
2 useful. And I don't know how many pages will be the report,
3 but clearly, there's material for quite a lot. So thank you
4 very, very much for coming, for your time, for sharing your
5 experience, expertise, and I really, really appreciate it.
6 Thank you.

7 --- Upon recessing at 12:30 p.m./

8 --- La séance est suspendue à 12 h 30

9 --- Upon resuming at 1:34 p.m.

10 --- L'audience reprend à 13 h 34

11 **COMMISSAIRE HOGUE:** Bon après-midi à tous.

12 This roundtable is entitled « Mise en œuvre,
13 dissuasion et poursuites des activités étrangères », or
14 "Enforcing, Deterring and Prosecuting FI Activities". And we
15 have with us four experts, and a fifth one is on the screen,
16 so we have five, actually, that we will hear from.

17 And it will be moderated again by Professor
18 Leah West.

19 **--- ROUNDTABLE : ENFORCING, DETERRING AND PROSECUTING FOREIGN**
20 **INTERFERENCE ACTIVITIES / TABLE RONDE: MISE EN OEUVRE,**
21 **DISSUASSION ET POURUITE DES ACTIVITÉS D'INGÉRENCE ÉTRANGÈRE:**
22 **--- PANEL MODERATED BY/PANEL ANIMÉ PAR DR. LEAH WEST:**

23 **DR. LEAH WEST:** Thank you, Commissioner.

24 Plusieurs aspects de l'ingérence étrangère
25 peuvent compliquer les enquêtes et les poursuites à
26 l'encontre de ses auteurs. Bien qu'il existe des lois qui
27 criminalisent certains types d'ingérence étrangère, il y a
28 relativement peu de poursuites pour ingérence étrangère.

1 Lors des audiences de Phase 1 au printemps,
2 la Commission a entendu des témoignages sur certains des
3 acteurs chargés d'enquêter et de poursuivre les infractions
4 liées à l'ingérence étrangère ainsi que sur certains des
5 défis auxquels ils sont confrontés.

6 Ces témoignages suggèrent qu'il y a des
7 importantes questions à poser pour savoir si les lois, les
8 procédures et les organismes d'application de la loi
9 canadienne sont conçus et dotés des ressources nécessaires
10 pour enquêter efficacement sur les activités d'ingérence
11 étrangère, les décourager et les poursuivre.

12 This raises numerous questions raised under
13 this theme, but I'm going to begin by asking all of our
14 panellists a single question, and then I'll introduce those
15 panellists.

16 And the single question I have is, is the
17 criminal law and criminal law process a sufficient, necessary
18 and appropriate way of deterring, detecting and countering
19 foreign interference, and are there reasons why other
20 approaches should be preferable?

21 To answer this broad question, we're joined
22 first by Mr. Bob Paulson, the former Commissioner of the
23 Royal Canadian Mounted Police, Professor Robert Currie at
24 Dalhousie University, Professor Alex Wilner, an Associate
25 Professor at Carleton University, Professor Michael Nesbitt,
26 an Associate Professor at the University of Calgary, and
27 online we have Mr. Croft Michaelson, who's the former senior
28 counsel for the Public Prosecution Service of Canada.

1 So I'm going to ask my colleague, Mr. Wilner
2 -- or Professor Wilner, I should say, to start with his
3 remarks.

4 **--- PRESENTATION BY/PRÉSENTATION PAR DR. ALEX WILNER:**

5 **DR. ALEX WILNER:** Thank you.

6 Dear Commissioner, distinguished guests,
7 fellow panellists and colleagues, there are three distinct
8 topics before us today, enforcement, prosecution and
9 deterrence, and I will focus my time on the last of these
10 three processes, deterring foreign interference.

11 Much of my scholarly research over the past
12 20 years has explored the ways in which classical deterrence
13 theory, as first developed by political scientists during the
14 Cold War, might be reimagined and reapplied against a range
15 of contemporary security challenges, and so I illustrate how
16 states might deter violent radicalization, transnational
17 terrorism and insurgency.

18 I also assess deterrence in cyberspace and
19 within the constructs of information warfare, and I explore
20 how artificial intelligence might both undermine and augment
21 military deterrence. And more recently, with a former PhD
22 student of mine, Dr. Marshall Palmer, I've proposed a more
23 expansive deterrence framework for application against
24 foreign election interference.

25 And so today I'd like to share my high-level
26 thoughts on two aspects of deterring foreign interference.
27 First, I will define the nature of and describe the
28 prerequisites for deterrence in countering foreign

1 interference. And second, I would like to illustrate the
2 various pathways in which deterrence by punishment, denial
3 and delegitimization might be applied against foreign
4 interference.

5 Though I am not a legal scholar, my comments,
6 I think, dovetail nicely with those of my fellow panellists
7 in that I describe the larger legal, domestic, geopolitical
8 and security contexts in which deterrence theory and practice
9 can be applied to counter foreign interference in this
10 country.

11 At its conceptual core, deterrence is
12 fundamentally about using a combination of threats to shape
13 an adversary's behaviour in a way that meets our own
14 objectives. It entails convincing another actor, who remains
15 able to behave in ways that are detrimental to us, to
16 willingly forego an action that we would rather they not
17 pursue.

18 There are two guiding principles in forming
19 my understanding of deterrence theory. First, deterrence is
20 not simply something that you say or casually lump together
21 with other related terms like defence or enforcement or
22 defeat. Rather, deterrence is a framework or a strategy, and
23 it's built on an understanding about the nature of behaviour
24 that can be applied to any context in which we seek to shape
25 or change another actor's behaviour.

26 And second, if deterrence is defined as
27 convincing an adversary to forego an unwanted action, then in
28 practice, deterrence rarely just happens on its own. Rather,

1 deterrence is something that you do and that you communicate
2 proactively.

3 Deterrence is the result of putting into
4 practice a strategy that seeks to manipulate, to shift or
5 alter an adversary's behaviour in ways that meet our own core
6 objectives.

7 So I would like to encourage, first, that
8 members of the Commission use the term diligently and
9 consistently to refer to a larger framework in which Canada
10 leverages a combination of threats and defences in a way that
11 convinces foreign actors who means us harm to pursue -- not
12 to pursue foreign interference and related activities.

13 Now, there are several prerequisites
14 informing the strength and utility of any deterrence
15 framework. The first, deterrence involves at least two
16 actors. The first actor is known as the challenger, who
17 contemplates a particular course of action. And the second
18 actor is known as the defender, who seeks to deter that
19 unwanted action. Another way to think about these relations
20 is that a challenger wants to change a status quo
21 relationship while a defender seeks to uphold it. And so in
22 our particular case, Canada is the defender and foreign
23 actors contemplating interference are the challengers.

24 Second, a deterrence framework should seek to
25 weigh on a challenger's cost-benefit analysis. Rational
26 behaviour is predicated on the costs or effort an action is
27 assumed to entail against the benefits or gains the action is
28 assumed to generate. When a rational actor believes that the

1 benefits -- sorry, that the cost of its actions outweigh the
2 perceived benefits, deterrence theory speculates that it
3 should forego a ---

4 **MS. LEILA GHAAHARY:** Excuse me ---

5 **DR. ALEX WILNER:** --- particular action ---

6 **MS. LEILA GHAAHARY:** --- Mr. Wilner, could I
7 ask you to slow down ---

8 **DR. ALEX WILNER:** I'm sorry, yes.

9 **MS. LEILA GHAAHARY:** --- for the
10 interpreters, please. Thank you.

11 **DR. ALEX WILNER:** As a prerequisite to
12 deterrence, our challengers must be sufficiently swayed by
13 rational choice.

14 A third prerequisite, defenders must clearly
15 communicate threats, readiness and expectations to
16 challengers, such that adversaries absorb relevant
17 information, they consider how to respond, and then they
18 inform or change their behaviour. Communication is critical
19 to deterrence. A threat that is unmade or a warning that
20 isn't heard or properly understood will fail to generate the
21 desired coercive effect on our adversaries.

22 A fourth prerequisite, defenders must have a
23 perceived capability to act as they have threatened and to
24 demonstrate a resolve to act as threatened if and when
25 required. Bluffing undermines deterrence. A challenger must
26 believe that a defender can and will act as it has
27 communicated.

28 And finally, deterrence works best against a

1 known adversary. Anonymity in either physical or digital
2 space complicates how deterrence is communicated and carried
3 out. Attribution is an important consideration when
4 identifying our challengers.

5 So let me turn next and conclude by putting
6 all of these definitions, concepts and prerequisites together
7 within the context of deterring foreign interference in
8 Canada.

9 Three deterrence pathways present themselves:
10 punishment, denial and delegitimization. Deterrence by
11 punishment promises some form of retaliation if a challenger
12 pursues an unwanted action. Punishment adds to an
13 adversary's costs, potentially tipping the scales of a cost-
14 benefit calculation towards inaction. Deterrence by denial,
15 conversely, functions by subtracting from or diminishing an
16 adversary's perceived benefits. Here our goal is to deny a
17 challenger what it seeks from a cost-benefit perspective.
18 Denial creates a cost by promising failure. If an adversary
19 is convinced that the unwanted action in question is unlikely
20 to get them what they desire, they may be less willing to
21 try.

22 And then finally, deterrence by
23 delegitimization. This functions by informing and shaping an
24 adversary's beliefs, attitudes, ideologies and other
25 motivating factors. Delegitimization turns on social
26 pressure and perceptions of right and wrong. In this case,
27 challengers are deterred from pursuing a certain behaviour
28 when the behaviour itself generates a belief, or a perception

1 within the actor, or among its stakeholders that pursuing the
2 unwanted action would be shameful, disgraceful, or
3 detrimental to the larger objectives.

4 A Canadian deterrence framework for
5 countering foreign interference should combine elements of
6 all three processes. The framework would provide the
7 conceptual backbone for combining the disparate approaches to
8 counter interference under one guiding conceptual rubric of
9 deterrence. And moreover, this framework would tie the
10 various approaches and solutions that Canada and other
11 democracies are proposing and applying to countering foreign
12 interference within a larger overarching strategy.

13 Now importantly, that strategy itself could
14 be broken down and applied to different actors involved in
15 foreign interference, so state and non-state sponsors of
16 foreign interference and Canadians, foreign nationals and
17 domestic organizations involved in its promotion can be
18 punished. The effect that interference is meant to have on
19 Canadians, on our society, on our democratic processes can be
20 denied. And bolstering democratic norms, values, principles,
21 expectations and institutions, both at home, but also abroad
22 might delegitimize the acceptance or use of foreign
23 interference among a variety of stakeholders, from elected
24 officials to individual voters.

25 So let me conclude then with a scenario that
26 breathes life into the proposed deterrence framework. Heavy
27 and open investments in Canada, in Canada's ability to
28 successfully investigate, enforce and criminally prosecute

1 domestic and foreign individuals, organizations and corporate
2 entities promoting foreign interference in Canada would occur
3 under public and journalistic scrutiny. Concurrently,
4 Canadian officials working lockstep with our democratic
5 allies could issue a more nuanced and credible series of
6 threats to punish state sponsors of interference, including
7 by threatening sanctions and public exposure and, possibly,
8 at the very extreme end, by threatening military or cyber
9 retaliation for interference that is deemed a threat to
10 critical national infrastructure.

11 Elsewhere, applying a whole of society
12 approach to countering interference would deny its purpose
13 and diminish its utility. In this case, different levels of
14 government would work with the federal government to limit
15 and constrict the intended effects of foreign interference by
16 diminishing the scope and perhaps the reach of
17 disinformation, by encouraging or forcing private sector
18 partners to scrub disinformation from their platforms, and by
19 improving Canadian cyber security practices in ways that
20 diminish the theft of sensitive information that might be
21 repurposed to influence our elections and elected officials.
22 And by way of public and formal education campaigns, our
23 society's ability to identify and ultimately ignore
24 disinformation meant to interfere with our democratic
25 processes might be strengthened.

26 Finally, clearly and repeatedly discrediting
27 foreign interference domestically and internationally as a
28 disgraceful form of behaviour by championing democratic norms

1 and institutions might, among and within certain societies,
2 but also including our own, create social costs to
3 participating in foreign interference. If interference is
4 widely interpreted as shameful, would-be local politicians at
5 all levels of government may become less inclined to accept,
6 invite or welcome foreign interference on their behalf. And
7 doing so would be counter to what they believe is just and is
8 expected of them.

9 So, in sum, criminal law is a necessary but
10 not sufficient means of deterring foreign interference in
11 Canada. Deterrence entails a complex interaction between
12 different actors and processes that encourages a more nuanced
13 understanding of our adversary's cost-benefit calculations in
14 deciding whether, when and how to interfere in Canada.
15 Crucially, deterrence theory helps by identifying the tools,
16 the technology, the infrastructures, the processes needed to
17 manipulate and shape our adversary's calculus and preferences
18 by weighing on and utilizing punishment, denial and
19 delegitimization together. Thank you.

20 **COMMISSIONER HOGUE:** Thank you.

21 **DR. LEAH WEST:** Thank you, Professor Wilner.

22 Mr. Paulson?

23 **--- PRESENTATION BY/PRÉSENTATION PAR MR. BOB PAULSON:**

24 **MR. BOB PAULSON:** Well, good afternoon,
25 everyone, Commissioner. Thanks for the opportunity to
26 participate in the Commission's important work. I'm of the
27 view that a properly resourced, *Charter* compliant,
28 professionally aggressive criminal investigation leading to a

1 timely and successful prosecution is an essential component
2 of Canada's so-called all of society approach to foreign
3 interference. That said, I think we need to recognize that
4 hostile state actors are unlikely to stop their activities
5 because we successfully arrest and prosecute their proxies or
6 confederates. In short, we're not going to arrest our way
7 out of this. We must, however, demonstrate competency and
8 timeliness in bringing the criminal justice system to bear
9 against those who would give life and participate in this
10 criminal interference.

11 Arrest, charges and ultimately convictions, I
12 believe, crystalize in the mind of Canadians the true nature
13 of the threat that we face and it's an opportunity to
14 demonstrate what I think Canadians expect with some
15 accountability for what they're hearing about.

16 There are a number of actors in this for
17 God's sake's do something about this area, and they're all
18 armed with a host of powers and authorities and enforcement
19 options. CSE, CSIS, RCMP, Global Affairs, Elections Canada,
20 the Commissioner of Elections, other government departments.
21 And now, a Commissioner of Foreign Interference and
22 Transparency.

23 There already exists a fair number of
24 criminal offences which the police could rely upon to bring
25 enforcement against some of these activities. Some of them
26 include extortion, breach of trust, corruption, and
27 particularly relevant perhaps to transnational repression is
28 the offence of intimidation and threatening.

1 Now it's bolstered by the provisions of C-70,
2 which include some relatively complex new offences, but
3 again, some additional authorities.

4 So here we are with a complex array of
5 security and intelligence agencies and enforcement bodies, a
6 complex array of authorities, and powers, and enforcement
7 options. And so what I say is need is some coherence in
8 decision-making around what to use when. And that's easier
9 said than done, I'm sure you've started to appreciate.

10 So let me talk about the decision to initiate
11 and pursue a criminal investigation, largely understood to be
12 the prerogative of the police, and mostly that's true.

13 You know, a solid belief or a threshold
14 belief, and a specific criminal act in my view, imparts a
15 duty on the police to act, to investigate, to bring charges,
16 or recommend charges, and support a prosecution.

17 But there's also the -- and so that seems to
18 alienate the police somehow from many of the discussions
19 around grand policy options in attacking this problem. But
20 what's available to the police and to the broader community
21 that I've described is this idea of police discretion.

22 So let me take you back to the earlier 2000s
23 when terrorism was as bad as it ever was and we were having
24 difficulty bringing successful prosecutions against those
25 that were identified as posing a threat to Canadians through
26 the intelligence system.

27 CSIS and the RCMP put their heads together
28 and were able to dovetail their efforts in the form of what

1 was called and what is called One Vision. I believe it's up
2 to 3.0 now. But it's a series of principles, and it's rather
3 significant in that before then, it turned on the sort of
4 relative enlightenment of the leaders of each agency, which
5 didn't happen very often. And so this structured governance
6 system permitted decision-makers in both organizations to
7 look at specific cases and to apply some principles in
8 coordinating their efforts. Things like a criminal justice
9 response is the desired response, is the preferred response
10 when there's a threat to public safety. Things like a
11 prescribed cadence of operational deconfliction meetings.
12 Things like adopting the principle that when a criminal
13 justice response is anticipated, the earlier the information
14 is transmitted to the police, the better. A series of things
15 all contemplated and deployed to try and get ahead of this
16 seemingly insurmountable intelligence-to-evidence obstacle.

17 And it's successful. I think we can point
18 objectively to many successes of that approach.

19 And I think a similar approach, building
20 perhaps on the seed of the SITE Task Force, but broader, to
21 include many of these agencies, with some specific governance
22 around interacting, around keeping political considerations
23 out of discussions, around strategies and options, given the
24 circumstances as they're presented in each individual case,
25 with a principle of acting versus spreading information.
26 Acting versus knowing. That's fundamentally the difference
27 between the intelligence world and the enforcement world.

28 When you get all these people together, there

1 could be discussions like recognizing that perhaps a criminal
2 investigation of transnational efforts to threaten people at
3 home are legitimate and likely to occur, and therefore a
4 criminal prosecution or a criminal investigation is probably
5 not the best way to proceed and there may be other options.
6 But there's got to be a way of preserving those decisions and
7 the rationale that goes into those decision-making exercise.

8 Lastly, I'll just talk -- and no discussion
9 of criminality would be complete without a discussion of
10 resources.

11 I had the opportunity years ago to speak at a
12 forum on something called the economics of policing. And I
13 was able to do a little bit of research in terms of public
14 spending per capita on health, on education, and on policing.
15 On the first two, there was essentially an X equals Y graph
16 that demonstrates the investment, public investment, in those
17 two areas. Whereas policing kind of horizontally crept
18 across the page.

19 Park that for a second, but juxtapose it
20 against the evolution of the *Charter*, and trying to conduct
21 *Charter*-compliant investigations imposes an enormous
22 logistical task on police agencies and requires a different
23 approach to project-based attacks on -- particularly on
24 people who don't want to be caught. Particularly on people
25 who anticipate a criminal justice response.

26 Federal policing, which is the area generally
27 that has conduct of this in the RCMP, is woefully
28 underfunded. And contrary to a lot of public discussion,

1 it's not because the RCMP is involved in contract policing,
2 because the contracts pay their own freight, essentially. A
3 contracting province or municipality pays for what they get.
4 It's an actual cost contract.

5 But federal policing has been engaged in an
6 enormous remit of responsibility in terms of
7 counterterrorism, national security, in terms of drugs and
8 organized crime, border enforcement, financial crime,
9 protective policing has come under pressure lately, and
10 international policing.

11 So to think that, you know, you're going to
12 get a highly competent investigative response that is going
13 to be able to position enforcement in a way that gives life
14 to some of the things I said, would require an enormous
15 investment in a regionalized approach to deploying these
16 teams of investigators and specialized support and
17 administrative support.

18 I mean, what used to be a two-to-three
19 paragraph justification for a search and seizure instrument
20 when I was a constable is now a two-to-300-page document.
21 The -- and God help the investigator that has a failure to
22 disclose relevant information in that ITO.

23 So it's a very high-risk enterprise.
24 Disclosure costs are through the roof.

25 So I would just add that, in close, on the
26 need to take this seriously, the need to recognize that
27 enforcement is a component of our response, but the need to
28 make sure that we have the capacity to deliver *Charter-*

1 compliant investigations.

2 Thank you.

3 **COMMISSIONER HOGUE:** Thank you.

4 **DR. LEAH WEST:** Thank you.

5 Mr. Michaelson?

6 **MR. CROFT MICHAELSON:** Thank you. Good
7 afternoon. Can you hear me?

8 **DR. LEAH WEST:** Yes, we can.

9 **--- PRESENTATION BY/PRÉSENTATION PAR MR. CROFT MICHAELSON:**

10 **MR. CROFT MICHAELSON:** Okay. That's great.
11 Thank you very much for the invitation to participate on this
12 roundtable.

13 I was a federal prosecutor for almost 30
14 years, and in senior general counsel with the Public
15 Prosecution Service of Canada and my remarks are rooted in my
16 experience as a prosecutor, in particular my experiences
17 conducting prosecutions raising sensitive national security
18 issues.

19 In my view, the criminal law has an important
20 role to play in signalling to foreign states and their agents
21 the types of conduct that we consider unacceptable, but I
22 would caution against relying on the criminal law to do much
23 of the heavy lifting in combating foreign interference.

24 Other measures outside of the criminal law,
25 such as administrative proceedings under the *Foreign*
26 *Influence, Transparency, and Accountability Act*, sanctions,
27 enhanced governance and oversight of vulnerable processes may
28 well be more effective than criminal proceedings in deterring

1 foreign interference.

2 I see three challenges with using criminal
3 law to combat foreign interference.

4 The first is the challenge of defining
5 foreign interference offences with sufficient precision to
6 survive scrutiny under the *Charter*. The second is the high
7 bar required to obtain a conviction at a criminal trial. And
8 the third is what is commonly referred to as the
9 intelligence-to-evidence problem, the difficulties that arise
10 when one seeks to use intelligence information in the context
11 of criminal investigations and prosecutions.

12 Turning to the first challenge, the challenge
13 in defining criminal conduct with sufficient precision. Both
14 you, the Commissioner, and the National Security and
15 Intelligence Committee of Parliamentarians have noted the
16 difficulty in drawing a line between foreign influence that
17 is considered legitimate and foreign interference that is
18 unacceptable, and you both observed that there is a
19 considerable grey zone.

20 The point I wish to make here is that the
21 criminal law itself is not a particularly good tool to try to
22 address ambiguity or conduct that may fall into a grey zone.
23 Criminal offence provisions are subject to scrutiny under the
24 *Charter of Rights and Freedoms* for overbreadth, and the
25 Supreme Court of Canada has stated that if a criminal offence
26 provision is so broad in scope that it includes conduct
27 bearing no relation to the law's purpose, that provision will
28 be overbroad and violates section 7. This places a restraint

1 on the use of the criminal law. Laws that are broadly drawn
2 to make enforcement more practical will run afoul of section
3 7 if they deprive even one person of their liberty in a way
4 that does not serve the law's purpose.

5 Now, the new foreign interference offences in
6 the *Foreign Interference and Security of Information Act*
7 appears to have been crafted with this principle in mind, and
8 they seem to capture much conduct that is considered foreign
9 interference, but could one go further and craft a broader
10 offence or offences that would capture all of the potential
11 permutations of foreign interference? I'm not sure that one
12 could do so without running into serious concerns of
13 overbreadth.

14 Turning to the second challenge associated
15 with using the criminal law, the legal standard to prove a
16 criminal case is high. The Crown is required to prove all of
17 the elements of the offence beyond a reasonable doubt, a
18 standard considerably higher than the civil standard of proof
19 on the balance of probabilities.

20 I note that the new foreign interference
21 offences all require that the Crown prove a link between the
22 offender and a foreign entity. The Crown must typically
23 prove beyond a reasonable doubt that the offender engaged in
24 certain conduct at the direction of, in association with, or
25 for the benefit of a foreign offender.

26 Practically speaking, I think that this
27 particular element will be the most challenging for the
28 police to investigate and for the Crown to prove in a

1 criminal trial proceeding. Given that we are talking about
2 conduct by foreign entities and their agents that is designed
3 to be concealed and obscured, you can anticipate that it will
4 be quite difficult for the police go gather sufficient
5 evidence to prove the link with the foreign entity beyond a
6 reasonable doubt. The high bar to prove a criminal
7 conviction lessens the utility of the criminal law as a tool
8 in deterring foreign interference.

9 I'll turn now to the third challenge, often
10 referred to as the intelligence-to-evidence problem, which
11 relates that the difficulties one encounters when one seeks
12 to bring intelligence information obtained through covert
13 means into a criminal trial process that is open and
14 transparent.

15 I think it likely that future investigations
16 of the new foreign interference offences will have their
17 genesis in intelligence information that is shared by CSIS
18 with the police. This is because one of the essential
19 elements of the offence, that necessary link between the
20 offender and the foreign entity, will probably first surface
21 in the context of an intelligence investigation. In my
22 experience, the intelligence investigation gathered by CSIS
23 that is likely to have particular value to a police
24 investigation is likely to consist of information from either
25 confidential human sources or intercepted communications, and
26 there are difficulties associated with relying on both types
27 of intelligence.

28 If the intelligence information is from a

1 confidential human source, that will pose a difficulty
2 because both the human source and the Service would need to
3 agree to waive the confidentiality that ordinarily protects
4 the identity of the human source under the *CSIS* Act. That is
5 a not to say a waiver of confidentiality is out of the
6 question. In the Toronto 18 terrorism case, two confidential
7 *CSIS* sources agreed to become police agents and testify at
8 trial. But human sources in this particular context may be
9 reluctant to disclose their identities if they have concerns
10 about possible retaliation by the foreign entity against
11 themselves or their loved ones.

12 If the intelligence information provided to
13 the police is a communication intercepted under a *CSIS*
14 warrant, and the police then rely on that communication as
15 part of the reasonable grounds to obtain their own warrant or
16 authorization to intercept communications, the *CSIS* warrant
17 and underlying affidavit may well become the subject of
18 scrutiny at trial.

19 The trial court may well need to review the
20 *CSIS* warrant and affidavit to determine whether the seizure
21 of the communication by the Service was lawful. That's an
22 important consideration any time the product of a *CSIS*
23 warrant issued by the police is whether that warrant and
24 affidavit could be disclosed to the defence in a manner
25 sufficient to allow for effective review and challenge at
26 trial without compromising national security.

27 In some cases it will be possible to balance
28 these two competing interests. A good example of this is a

1 terrorism case that I prosecuted, *Regina versus Jaser*, where
2 we were able to provide the defence with redacted copies of
3 the CSIS warrant and underlying affidavit, as well as
4 summaries of redacted information in a manner that was
5 sufficient to allow for effective review and challenge at
6 trial. And in that case, the trial judge was able to
7 conclude that the CSIS warrant was lawful, but there may well
8 be other cases where it will not be possible to disclose the
9 warrant and affidavit in an redacted form that is sufficient.
10 And if that is the case, the information gathered under the
11 warrant could not be used by the police.

12 I should add that in *Regina versus Jaser*, the
13 Service provided redacted copies of the warrant and
14 affidavit, and some summaries of redacted information in
15 consultation with both the prosecutor, myself, and the trial
16 judge, but without the involvement of the Federal Court. In
17 that case, the defence was content with what the Service
18 produced. But in other cases, the defence might well resort
19 to the section 38 disclosure regime in the *Canada Evidence*
20 *Act*, and pursue an application in the Federal Court for
21 disclosure.

22 In my view, the section 38 disclosure regime
23 is both cumbersome and time-consuming. If the defence had
24 resorted to that process in *Regina versus Jaser*, it would
25 have resulted in the bifurcation of the proceedings and
26 likely contributed to considerable delay of the trial.

27 In summary, Commissioner, the foregoing
28 challenges associated with the criminal law, in my view,

1 limit its utility in combatting foreign interference, and
2 other measures that don't have these same challenges may well
3 be more effective.

4 Thank you.

5 COMMISSIONER HOGUE: Thank you.

6 DR. LEAH WEST: Professor Nesbitt.

7 **--- PRESENTATION BY/PRÉSENTATION PAR DR. MICHAEL NESBITT:**

8 DR. MICHAEL NESBITT: Thank you, and thank
9 you for the opportunity to be here, to the Commissioner and
10 everyone involved.

11 In some ways I'm going to skip the beginning
12 of what I had to say and echo the comments of Mr. Paulson,
13 Mr. Michaelson, and Mr. Wilner, and just say that criminal
14 law is an absolutely necessary but clearly insufficient tool
15 in the toolkit to combat foreign interference. Obviously,
16 it's important that Canada is not seen as a safe haven where
17 this sort of activity can take place. On the other hand,
18 criminal law, when applied, will only be applied to a small
19 handful of cases at any given time, and within that, a small
20 handful of the types of activities and the manifestations
21 that might result from foreign interference. So in other
22 words, a small subset of a small subset of the larger foreign
23 interference pie.

24 So what I'd like to focus on, instead of the
25 criminal law as we often think about it, which is the
26 offences, I'd like to talk about criminal process, procedure,
27 and structures. I think that is -- and haven't come up with
28 a better word for it, but this is a little unfair, but I'm

1 going to say where Canada has tended to fall down, when it
2 has fallen down, tends to be on the enforcement side of
3 existing laws, not the absence of laws in this area, and
4 particularly after Bill C-70 and some of the recent new laws
5 we have in this area, I think we have more than enough in
6 general on the criminal law side on the books in our *Criminal*
7 *Code* and security so, yeah.

8 What I think then is Canada needs to focus on
9 the effect of investigation of criminal laws, as you've
10 heard, and that is to say bringing them to charge and then to
11 a successful, fair and, as Mr. Paulson said, *Charter*
12 compliant result. But I also think this means thinking a
13 whole lot bigger than tinkering. That doesn't mean tinkering
14 with offences. It doesn't mean tinkering with bureaucratic
15 processes that are already in place. It doesn't mean
16 tinkering to get us to a One Vision 4.0. All of that may be
17 necessary, but again, it is insufficient, and at this point,
18 it probably amounts to tinkering around the margins.

19 So I'm going to focus on two institutions in
20 particular and one subject area that require a good deal of
21 work and a good deal of big thinking, the first being the
22 RCMP, the second being CSIS, and the third, this is subject
23 matter area and I'll call it money crimes, broadly speaking.
24 In each case, I'm going to focus not on the offences or the
25 particular mandate that they have, but rather, on the big
26 picture, so the institutions, the processes and the
27 resourcing that will drive the investigations.

28 Okay. First the RCMP. As I know this

1 Commission has now heard, Canada's RCMP is bifurcated, a
2 term, by the way, that very much defines this area of law.
3 It is bifurcated between national security policing and
4 contract policing. That bifurcation happens the moment
5 someone walks in the door to be trained, continues through
6 promotion, and then on to the skills that are developed and
7 maintained when the investigations take place.

8 I'm happy to answer questions here. I'm not
9 going to get into it in detail, so for now, I'll simply add
10 my name to what I think is a chorus of academics who have
11 studied this and perhaps what the Commission has already
12 heard, and that being that much of the RCMP's contrasting
13 [sic] policing agreements expire on or around 2032. And it
14 is time to start planning for the expiration of those
15 contracts now and what it will mean to proceed thereafter
16 with a true national police force.

17 The focus needs to be on structure and
18 resourcing here, where the money goes, why and what the
19 implications are. That includes how do you attract, train
20 and retain experts needed to do national security policing
21 correctly. So to put that in lay terms, how do you get a
22 forensic accountant away from KPMG that stays away from KPMG
23 when KPMG pays a whole lot more money. It is at this point
24 time to plan for something different with the RCMP.

25 Second CSIS. As you've already heard,
26 Canada's system of investigating national security matters
27 was bifurcated in 1984. It was bifurcated again between
28 those that collected intelligence but also some evidence,

1 that being CSIS, and those that collect evidence, of course,
2 but also, by the way, some intelligence, and that being the
3 RCMP. Before then, like perhaps the FBI, the RCMP collected
4 both. Now there were good reasons in 1984 to suggest a
5 separate intelligence agency, and I won't get into that
6 history. Nor am I saying there isn't good reason to have
7 both CSIS and the RCMP. What I am saying is that while the
8 day-to-day relationship between those two organizations has
9 been discussed time and time again and put into practice
10 through One Vision 1.0, and then 2.0, and that was imperfect,
11 and then 3.0 and that was imperfect, and within the next 5
12 years 4.0 and that's imperfect. What hasn't been discussed
13 is the broader structural relationship between these two
14 organizations and what exactly they're doing in this space.

15 So again, to give one example, we have CSIS
16 and the RCMP investigating a terrorism matter. At some
17 point, the RCMP will take over and start investigating to
18 charge. The question then becomes at court one about sharing
19 information, about whether they have stepped on each other's
20 toes in the process, the question that isn't being asked is,
21 why is CSIS still there? And there's good reasons for them
22 to still there; right? It's hard to pass this back and
23 forth; right? Maybe they want to keep an eye on things
24 beyond the police investigation. Maybe they're looking at
25 other factors in the investigation. There's also good
26 reasons for them not to be there. We're already paying
27 another organization to do this work, to lead to what the
28 goal is, which is prosecution, and that other organization

1 may be actually hampered by the disclosure regime that will
2 invariably result when you have multiple national security
3 organizations involved in that process. So it's time to
4 think about some of those broader structural relationships
5 between these organizations.

6 And I'm going to quote something which I
7 think is -- which I think has been improved but I think it's
8 important and this comes from a Toronto 18 or so-called
9 Toronto 18 terrorism trial from 2009 and that's *Ahmad*, and
10 this is a quote.

11 "CSIS was aware of the location of
12 the terrorist training camp. This
13 information was not provided to the
14 RCMP who had an undercover -- who had
15 to uncover that information by their
16 own means. Sometimes CSIS was aware
17 that the RCMP were following the
18 wrong person, or that they had
19 surveillance on a house when the
20 target of the surveillance was not
21 inside, but CSIS did not intervene."

22 (As read)

23 It's time to start looking about -- looking
24 at why that happens, how that information is shared at a
25 broader level.

26 Another area to consider is one you've again
27 heard about, which is the intelligence-to-evidence conundrum
28 and Canada, again, with our bifurcated court system between

1 the Federal Court and terrorism, or these sort of cases, the
2 Superior Courts.

3 This was first addressed in 2010 in the Air
4 India Inquiry, which essentially recommended an end to the
5 bifurcated system. As far as I know, every consultation we
6 have on this, which recently is every few years, have come
7 back with another suggestions which -- a number of
8 suggestions which are often taken up. And the one suggestion
9 that isn't taken up, for whatever reason, continues to be the
10 study of the bifurcated system. And I will say it's my own
11 sense that the recommendation with respect to the bifurcated
12 system from virtually anyone who studies it outside of the
13 institutions, right, so those who see the processes, those
14 who are not in Ottawa -- let Mr. Michaelson speak to
15 prosecutors who may be in the region and see this in a
16 particular way, but it's that it doesn't make any sense.

17 If -- to be clear about this, if Kafka were
18 writing today, Canada's bifurcated system in national
19 security matters would fit very well into the trial. He just
20 didn't manage to think of it. It's a hinderance, as Mr.
21 Michael said to speedy trials. It takes away from the
22 criminal process for what seems to me a largely uncertain
23 result.

24 One other thing I'll mention with respect to
25 CSIS, is there are some simple reforms, but again, they're
26 broader; right? So not a new criminal offence, but we should
27 be thinking about legislating O'Connor rules, so for third-
28 party disclosure with respect to national security

1 institutions or government institutions. So *O'Connor* was a
2 case that dealt with health information from the '90s, but
3 now it's being applied most often to information held by CSIS
4 as a third-party collector of intelligence with some overlap
5 to the RCMP. There are ways to legislate that could clarify
6 what those rules are and make it easier rather than fiddle
7 with processes of those trying to abide by current rules.

8 And I will just say, we have a couple of at
9 least academic papers on this which make a whole lot of
10 sense. One is by Craig Forcese and another is by Leah West,
11 and it's called "The Problem of 'Relevance': Intelligence-to-
12 Evidence Lessons from UK Terrorism Prosecutions" in the
13 *Manitoba Law Journal* 41(4) from 2018.

14 The final one I'll mention here is money.
15 And the money problem relates to CSIS and the RCMP, but we
16 also have to think about how it relates to the Public
17 Prosecution Service of Canada, Global Affairs, and others.
18 So in essence, do we have the right people with the right
19 skills and incentive hired in the right ways doing the right
20 work in the right places? And we have all sorts of evidence
21 to suggest we might have a problem here.

22 We have four sanctions prosecutions since
23 1991 in the history of Canadian sanctions law, and yet every
24 year we see Canadians prosecuted in the U.S. for violations
25 that look like they may violations in Canada, and we see
26 agencies from abroad saying Canada is a safe haven for this
27 sort of activity.

28 That's the same with terrorist financing. We

1 get criticized fairly regularly as Canada being a safe haven
2 for terrorism financing from a number of groups.

3 I'll give you one example. We've never had a
4 terrorist financing case with respect to money being sent to
5 Hezbollah. That's shocking if you know the Canadian system.

6 We have, I think, four charges out of the now
7 70 individuals charged, and we have multiple studies again
8 here, at least one I can think of, indicating that a number
9 of these cases could have gone ahead with terrorist financing
10 charges as well as what was charged, and it wasn't.

11 So again, the issue here comes back to the
12 broader question about resourcing of CSIS, of the RCMP, of
13 the right prosecutors. It comes back to questions as to why
14 the U.S. runs its sanctions, for example, out of the Treasury
15 Department and OFAC in particular, who are experts in
16 financing, and money, and spreadsheets, and all that sort of
17 stuff, and yet Canada continues to run it out of Foreign
18 Affairs, where diplomats move in their job every couple of
19 years and are not trained for any of this work.

20 But what comes from all of this to my mind is
21 a need to think big at this stage and make big
22 recommendations, not small tinkering. We need to think about
23 how the criminal law works. We need to think about the
24 structure of our national security organizations in relation
25 to existing laws. We need to think about how investigations
26 to prosecutions run through the system and how it's all
27 functioning together. We need to think about the resourcing,
28 but again that's not just the resourcing in terms of money,

1 that's also resourcing in terms of human resourcing, how you
2 do that, what the structure looks like of an organization so
3 that when money goes in, it doesn't get diverted two years
4 later to whatever the hot issue is that day.

5 Thank you.

6 **COMMISSIONER HOGUE:** Thank you.

7 **DR. LEAH WEST:** Small problems.

8 Professor Currie?

9 **--- PRESENTATION BY/PRÉSENTATION PAR MR. ROB CURRIE:**

10 **MR. ROB CURRIE:** Thank you, Dr. West.

11 Commissioner, Colleagues, I'm honoured to be
12 asked to appear today.

13 You've heard a lot of wisdom from my
14 colleagues. I'm going to drill down on the foreign part of
15 foreign interference and confine my remarks to one basic
16 theme, which is this: if the criminal law is to be used to
17 fight foreign interference, and I agree with the general
18 tenor of my colleagues' remarks, that it is a tool in the
19 toolbox, then it should be done with an explicit textured
20 focus on the international aspects of this situation that we
21 find ourselves in.

22 That is to say, our criminal law should be
23 used with the international context in mind. It should be
24 used in a way that's fully infused by relevant international
25 law norms, and specifically Canada's rights and obligations
26 under international law.

27 The nature of the threat here means that
28 criminal law, as a tool, needs to be employed in such a way

1 that it is fully protective of Canada's national interests in
2 an international setting where they are increasingly
3 threatened. And I will use my few minutes to explain what I
4 mean by all of that.

5 My starting point is that international law
6 is relevant to criminal law and it's more relevant today than
7 ever. And I start there because after more than two decades
8 of trying to teach this material to various players in the
9 justice system, I can assure you that most police officers,
10 criminal lawyers, and judges in Canada have little to no
11 working knowledge of the concepts I'm about to explain,
12 present company excluded, of course.

13 Encouragingly, the Prime Minister recently
14 invoked Canada's sovereignty. Sovereignty is one of the
15 bedrock principles of international law. It captures the
16 idea that states like Canada are fully independent entities.
17 Even in a state like Canada which is enriched and influenced
18 by other cultures and diaspora communities, our government
19 and our legal system make the decisions.

20 Right alongside the principle of state
21 sovereignty is the principle of non-interference. Foreign
22 states are not permitted to interfere with Canada's domestic
23 interests, nor can Canada do likewise to them.

24 To do so is to breach a fundamental norm that
25 is designed to allow countries to live in a state of
26 relatively peaceful coexistence. This international law rule
27 in part is why this proceeding is called the Foreign
28 Interference Inquiry.

1 The Prime Minister also recently mentioned
2 Canada's territorial integrity. In international law, a
3 sovereign state has a defined territory with borders and
4 despite the verbiage one hears about the increasing
5 meaninglessness of territory and the so-called borderless
6 world, territory is not obsolete and borders are not
7 obsolete, both matter.

8 On a country's territory, only the state can
9 act like the state. On Canada's territory, only the
10 government of Canada can make and invoke the force of the
11 law. This is particularly relevant to criminal law.
12 Criminal law has always been seen to be one of the areas of a
13 country's law that is closest to the heart of its
14 sovereignty, not just in Canada, but in all countries. And
15 it's often described as an expression of a country's
16 collective morality, but it has four other functions that I
17 want to briefly touch on. And I'll go lightly because my
18 colleagues have covered off some of it well. But they are
19 these four: a deterrent function; a protective function;
20 third, a communicative function; and fourth, an
21 accountability function.

22 On deterrence, a number of my colleagues have
23 spoken to this and I agree that the deterrent aspect of
24 criminal law is something we know about. And in this
25 setting, it should be engineered, and applied, and policed in
26 a way that it deters foreign actors from engaging in criminal
27 conduct on our soil. I agree with what I've heard here
28 today.

The final way in which Canada should use

1 criminal law is as an accountability mechanism. And I mean
2 something a little different than what Mr. Paulson meant,
3 though I agree with his remarks.

4 Contrary to popular belief, international law
5 is enforceable by various means that exist along the spectrum
6 from informal to formal.

7 States do take each other to court, to
8 international courts even. Canada itself is currently party
9 to proceedings against several foreign states at the
10 International Court of Justice.

11 To be sure, criminal law is not directly part
12 of those kinds of proceedings, which operate at the state-to-
13 state level, but my point is that the way in which we create,
14 administer, and enforce our criminal law should be done with
15 an awareness that it might eventually end up as part of an
16 international case. It should communicate that there's not
17 only the prospect of local criminal accountability for
18 individual actors, but also the prospect of international
19 accountability for foreign states that emerge as bad actors.

20 The prosecutorial charging decisions that are
21 made, the selection of evidence that is gathered, the
22 decisions to go to trial, the sentences that are imposed, all
23 of this should operate in appropriate cases with the
24 international context in mind, and the justice system and its
25 players need to have the knowledge and the toolboxes
26 necessary to factor this in in the right cases.

27 On that point, I'll conclude with a few
28 practical observations and proposals.

1 Because the context of the criminal acts
2 we're discussing here is so internationalized, it's important
3 that Canada maximise the use of the powers and the tools that
4 are at its disposal, and these tools can involve
5 international law, and in fact international law can make
6 them even more effective.

7 Here is one way. Police and Crown
8 prosecutors must become comfortable with the use of extended
9 territorial jurisdiction, which means charging and
10 prosecuting people for criminal acts that don't take place
11 entirely within Canada, or even maybe at their heart outside
12 of it, but which have impacts on Canadian territory, and
13 specifically that impact the lives of people in Canada.

14 We need more comfort with extraterritorial
15 jurisdiction, which is where we would be willing to prosecute
16 offences that take place wholly outside Canada, but are
17 linked to Canadian interests, very internationalized
18 interests.

19 Now, I say this not because you couldn't pick
20 up a text book and find it, because you can, but historically
21 there has been a reticence by Parliament in its lawmaking,
22 and the Crown and its law enforcing to fully engage on cases
23 that have international aspects. It's cultural and it's
24 unnecessary because international law is actually quite
25 permissive on these points. States are very free to take
26 jurisdiction over cases that affect their national interests,
27 even when those cases have transnational features.

28 Now, I do want to offer there's good news in

1 Bill C-70 and the changes that have been made. There is some
2 use of extraterritorial jurisdiction in there. Not as much
3 as is available, I think, but there is some. In any event,
4 everyone needs to understand it, both how it works and the
5 potential that it might cause upset that there are
6 international implications to how we manage this as well.

7 Of course, this is best done in active
8 collaboration with other states, which brings me to a second
9 point. Our Departments of Justice and Global Affairs, as
10 well as the RCMP's international cooperation bureaus, are the
11 contact points for our law enforcement partners in other
12 countries. They do good work. They facilitate Canada's
13 collaboration with a wide variety of foreign partners well
14 outside the Five Eyes. Canada has an extensive network of
15 criminal cooperation. But this network of cooperation
16 between countries needs to trickle down more into the local
17 law enforcement context more than it does currently.

18 Anecdotally, police and prosecutors the
19 country over will often quickly abandon cases that have
20 transnational aspects because they are viewed as being too
21 time consuming and administratively unwieldy.

22 In my home province of Nova Scotia, we've --
23 over 15 years, we've had a series of cases of foreign states
24 interfering in our criminal justice system, and what attempts
25 were made to deal with it were so far not successful, either
26 because of local unwillingness to engage with the
27 international aspects, or federal unwillingness to help when
28 they did.

1 Moreover, a lot of law enforcement personnel
2 are not necessarily aware of what international cooperation
3 networks are or how they can access them.

4 Cooperation even with our partner countries
5 can be bumpy and not all of that is easily fixed, but what we
6 can do is ensure that there is more effective circulation and
7 communication of information that makes policing and
8 prosecuting of transnational cases more informed and more
9 effective.

10 And on the policing side, it's important that
11 this does not begin and end with the RCMP. Policing of
12 matters with transnational aspects will often ultimately fall
13 into federal policing, but it's the front-line provincial and
14 municipal police who will frequently encounter these cases
15 first.

16 Particularly when interacting with diaspora
17 communities, especially those known to be targeted by foreign
18 states, police need to be able to be equipped to go into the
19 situation with an expectation that any criminal cases that
20 emerge will have transnational aspects, and therefore that
21 they will need to have knowledge, and skills, and access to
22 networks that are unconventional to their normal day-to-day,
23 but that will enable more success.

24 It's worth noting that there are encouraging
25 success stories in this regard, even just lately in the
26 media, like the RCMP's recent investigation revealed into
27 alleged activities by personnel and agents of a foreign
28 government.

1 What is needed, Commissioner, to conclude, is
2 a country-wide effort to enable police and prosecutors,
3 particularly in communities targeted by foreign interference,
4 to have the knowledge base and operational toolboxes to
5 ensure that Canada's criminal law can serve important
6 international objectives and more robustly protect Canadian
7 sovereignty.

8 Thank you.

9 **COMMISSIONER HOGUE:** Thank you.

10 **--- OPEN DISCUSSION/DISCUSSION OUVERTE:**

11 **DR. LEAH WEST:** So now I'm going to ask some
12 thematic questions of the panellists until we take the break.

13 I'll start by directing my questions to
14 individuals, and then ask for people to jump in as they see
15 fit.

16 And Professor Wilner, I'm going to put you a
17 bit on the spot, because we hadn't talked about this one, but
18 I'm going to ask you to assess your theory of deterrence and
19 your three criteria, and based on what you've heard, whether
20 or not you think our adversaries are deterred by Canada, and
21 why or why not?

22 **DR. ALEX WILNER:** They are not. And perhaps
23 not yet. What I'm fascinated by is the aspect of using
24 criminal law filtered through international law to signal
25 capabilities, intent, relationships. That's fascinating. I
26 think that's a useful way of putting the F back into foreign
27 interference. And so this is weaving the domestic space into
28 the international space.

1 I also would suggest that criminal law, or
2 law broadly, does signal normative red lines that we've
3 established, that we agreed upon that we will protect. That
4 sends a message again that we have our eyes open, at the very
5 least.

6 I appreciate Michael's point about a lack of
7 seeing through this; right? Seeing the end of it. Criminal
8 prosecutions. And this goes back to the terrorism issues
9 that we're faced with.

10 I think that sends the wrong message as well;
11 right? We have the laws, but we don't have the means to
12 pursue to the end, and so that may signal weakness.

13 And so I -- you know, I'm grappling with all
14 these issues. But I do think -- I think that we're perhaps
15 on the right trajectory towards adding new tools to the
16 toolkit that provides a fulsome approach to deterring and
17 countering foreign interference.

18 **DR. LEAH WEST:** Thank you. One of those new
19 tools in the toolkit is the Foreign Transparency Registry
20 that has not yet been put into full effect or practice.

21 But I'm wondering if, Mr. Michaelson, you can
22 think to its capacity to deter, in terms of do you think it's
23 going to be a good tool and are there ways of actually
24 enforcing it? Do you see it actually being enforceable?

25 And then I would just ask, Alex, if you think
26 that this kind of transparency mechanism does actually add to
27 its deterrent effect?

28 **MR. CROFT MICHAELSON:** Well thank you. So

1 with respect to the Foreign Transparency Register, it sheds a
2 light on activity, right, that currently is hidden. And when
3 we look at the experience in other countries, I mean, the
4 United States has had a Foreign Influence Registry for many,
5 many years. I think it goes back to the 1930s. You know,
6 their experience with it, until recent years, was that they
7 tended to sort of pursue voluntary compliance efforts, rather
8 than prosecutions.

9 I think part of the issue they had was that
10 they didn't have the power to compel documents and our
11 Foreign Transparency Register, the Commissioner will have the
12 ability to compel productions and documents.

13 Certainly our partners in the U.K. and
14 Australia have thought that this is a useful approach as
15 well.

16 So, you know, at the end of the day, we'll
17 see where it goes, but I think in terms of when you talk
18 about conduct, like, parliamentarians in particular, you
19 know, engaging in activity with foreign actors maybe they
20 shouldn't be engaged with. That will come to light. And I
21 think if those kinds of connections come to light, it will
22 have a deterrent effect, because people, I think, will be
23 less likely to engage in that kind of behaviour if it's going
24 to be public notice and quite open, published on a public
25 registry. So that's -- we'll have to wait and see how it
26 goes at the end of the day, but the ability of the
27 Commissioner to compel the production of documents, the
28 ability of the Commissioner to rely on information that is

1 not admissible as evidence in court proceedings, you know, it
2 seems like a good approach and a good first step, for sure.

3 **DR. ALEX WILNER:** I'm in general agreement.
4 I think the transparency registry does illustrate capability,
5 intent, resolve. I think the proof of use and the concept
6 itself would be to cross point a good marker for whether or
7 not it deters, but I think one issue, perhaps, that it -- or
8 one additional element is that it denies an easy route for
9 those willing to pursue foreign interference, an avenue to do
10 so.

11 And so going back to the concept of
12 deterrence by denial, we're not just looking to punish.
13 We're looking to deny easy access to do the bad things that
14 they want to do.

15 And so it's possible that this will do that.
16 Time will tell.

17 **DR. LEAH WEST:** One thing we heard in a panel
18 earlier this morning was the suggestion that even where
19 prosecutions may never happen because the individual is no
20 longer in the country, right, or we're talking about a
21 foreign agent that is abroad, there's a useful signalling
22 mechanism and a useful public education mechanism of bringing
23 charges for foreign interference even if there's no
24 reasonable prospect of conviction, which is generally the
25 threshold prosecutors use for bringing charges.

26 I'm just wondering if anyone has thoughts
27 about that, and I'll start with Mr. Paulson.

28 **MR. BOB PAULSON:** So I was fascinated by my

1 colleague's presentation on extra-territoriality, which is
2 something that we've availed ourselves of in the past. And
3 to your question, we charged a fellow by the name of Mokhtar
4 Belmokhtar in relation the kidnapping of Louis Guay and Rob
5 Fowler knowing fairly well and confident that we weren't
6 going to go and collect him from the Sahel and bring him back
7 to prosecution. And ultimately, I'm told -- I think we
8 learned that he's dead.

9 But to that very point, there is some benefit
10 in demonstrating the competency of the investigative
11 enforcement arm by bringing charges, and we've done it in
12 other cases successfully, bringing back one of the kidnappers
13 through an undercover ruse in the Lindo case, kidnapping
14 case.

15 So there is ample opportunity to bring -- and
16 Americans do it frequently, announcing charges against
17 Russian cyber attacks. Unlikely that they'll ever show up,
18 but if they do -- and I think that builds the confidence in
19 Canadians seeing that, actually, something is coming from it.
20 Maybe there will be no prosecution, but there's a record.

21 **DR. LEAH WEST:** Anyone else want to speak to
22 that?

23 Professor Currie?

24 **MR. ROB CURRIE:** Yeah, I agree entirely with
25 what Mr. Paulson said. There's a great deal of utility
26 there.

27 It's an activity for the police that requires
28 resources, it requires specialized knowledge, and that's

1 going to be a theme emerging here. Everything needs to be
2 well resourced and better resourced than it is, but that
3 signalling, communicative aspect is important. For Canada to
4 be out there in this way, it certainly underscores our
5 commitment to dealing with foreign interference, among other
6 kinds of criminal activities, and the -- you know, the simple
7 fact is Mokhtar Belmokhtar, people like that, we might never
8 get them or we -- I'm going to talk about Nova Scotia again.

9 We just had a case out of Nova Scotia
10 recently where a guy had jumped bail. We thought we'd never
11 see him again. He went to Italy for some reason. There was
12 an INTERPOL Red Notice issued, and they were waiting for him.
13 So that -- there's utility beyond the symbolic, I guess is
14 what I would emphasize there.

15 **COMMISSIONER HOGUE:** That will be a departure
16 from the -- I will say the common view or the way the various
17 agencies are operating these days. How would you suggest to
18 proceed for making such a shift in the way we are looking at
19 extra-territorial jurisdiction?

20 **MR. BOB CURRIE:** I'm more attuned to what's
21 going on with the Crowns and the courts, and so right there
22 I've long been an advocate for just more continuing legal
23 education on the international law aspects of domestic
24 criminal cases.

25 You know, the resources are available, but
26 when it's not part of the day to day very much, other things
27 rise to the top where it's more important that we look at,
28 you know, this other thing that we see more of and then, when

1 a relevant case comes up, there's a scramble for the toolbox.

2 And it's one thing if you're working in a
3 really well-resourced prosecution department in Toronto, but
4 entirely another thing if you're in Kamloops or Come By
5 Chance, Newfoundland, where you need to be able to get that.

6 So just making it part of the framework to
7 have resources available and ongoing training and familiarity
8 even if we're making people grit their teeth and bear it as
9 we introduce yet another thing for them to learn. And as --
10 and I don't mean to sound sceptical, but the fact of the
11 matter is, as I tell my students, there will never be less of
12 this, there will only be more. The world is getting smaller.

13 It's finally hitting Canada in a way that it
14 hit other countries long ago, and it's time that we increased
15 that capacity, I think.

16 **MR. BOB PAULSON:** I think if I can -- Bob
17 Paulson here, for the record.

18 If I can build on what Mike was saying
19 earlier, it turns on the professionalizing of the
20 investigative capacity, building, training, resourcing,
21 allowing that capacity to be deployed in those cases. In the
22 case of the Fowler-Guay kidnap, there was an enormous
23 government response because there was enormous public aspect
24 to the whole thing. And it seemed that, you know, having
25 those resources available already deployed and all sorts of
26 international activity, you know, warranted some sort of
27 outcome, some sort of result from this. The consequence of
28 kidnapping Canadians abroad was reinforced by quality

1 evidence given to the Attorney General to ultimately approve
2 charges.

3 But it turns on capacity and it turns on a
4 professional almost accredited approach to putting people in
5 charge of these investigations.

6 **DR. LEAH WEST:** So I want to turn now to
7 something that you recommended, which was this policy process
8 for thinking through options when it comes to activity that
9 might rise to the level of criminality and foreign
10 interference, but maybe criminal prosecution is not the
11 choice that we want to have.

12 And we heard from Professor Wilner that we
13 need a toolkit, and I think we've heard over the course of
14 the week that there is a big toolkit. We heard from our
15 diplomats about all of the different tools that they have in
16 their toolbox. There are sanctions. There's the
17 international legal forum, international fora. There's, you
18 know, pursuing intelligence threat disruption, cyber active
19 and defensive measures. Like there is a wide toolkit here,
20 but we need people around a table deciding which avenues to
21 pursue.

22 And I wanted to ask you to think through that
23 a bit more. You mentioned the lack -- or you need to have
24 those discussions without politics being at play, but for
25 most of the tools, other than choosing criminal prosecution,
26 there is Ministerial oversight required for any of them.

27 So I'm just wondering where you would sit
28 that body. Do you see multiple levels of some sort of

1 process, if you could think through that? And if anyone else
2 has anything they wanted to add on that as well.

3 **MR. BOB PAULSON:** So in my experience,
4 there's been clumsy efforts at trying to coordinate the
5 community. And this morning, you talked to two former very
6 well-respected National Security Advisors who talked about
7 the challenges of trying to coordinate the community.

8 It can't exist there because the political
9 considerations, although not, you know, sort of manifest in a
10 sense that Ministers aren't sitting around a table -- Deputy
11 Ministers are sitting around a table. And ultimately, this
12 becomes a political consideration.

13 So the success, if, indeed, we've had success
14 with the CSIS/RCMP evolution, has been to have practitioners,
15 operational practitioners, also agency leads, but operational
16 practitioners forced together to have discussions. I can
17 only imagine the kind of discussions that could be had given
18 the wide array of options that exist now. And in order to
19 arrive at the best course of action, I think they've all got
20 to be free to be able to discuss the possible consequences
21 outside of political considerations as to what may come of
22 PNGing a person rather than putting the handcuffs on them.
23 Or having CSIS do a threat reduction, if it's applicable.
24 The circumstances have to be, frankly, laid out for everyone
25 to be able to make those important decisions.

26 And there needs to be a record of those
27 discussions. Because I think some of the criticism that
28 we're hearing today is an absence of information about who is

1 making that decision? Who made that decision? And how did
2 that get reconciled, given the other responsibilities that
3 exist around government? So, I think it requires some heavy
4 thinking, but some clear, structured governance around those
5 assemblies of decision-makers within each of the agencies.

6 **DR. LEAH WEST:** Just a follow-up on that, to
7 think through practically, would you see foresee that coming
8 up with an options, you know, a list of options to pursue
9 that they would then be determined at the political level, if
10 it -- if those options required ministerial approval?

11 **MR. BOB PAULSON:** Well, ultimately, those
12 would be considerations in the discussion. If it was indeed
13 to rely sort of solely on a CSIS threat reduction activity,
14 then that requires ministerial engagement, and you would
15 recognize that. And what would be the consequence longer
16 term of engaging Ministers in that activity?

17 And, you know, a good example might be, I
18 heard colleagues talking about the registry. And I was
19 enormously excited to see the powers that this new
20 Commissioner would have to compel the so-called coercive
21 powers. Now, what -- as they're making decisions around
22 whether they'll proceed in an administrative fashion to
23 punish someone or refer it to the RCMP, what of the
24 information that's gathered and compelled, can that be
25 formed? Can that be relied upon by the investigation? And
26 how does that inform other agencies? They're very, very
27 complex issues that need those people in decision-making
28 roles to be able to do that, to make those decisions and

1 account for them.

2 But now, there's an absolute paucity of
3 accountability at any of these existing, you know, Assistant
4 Deputy Minister meetings and Deputy Minister meetings.
5 There's lots of discussion, lots of, "Okay, well, I'm going
6 to take that back." And there's no -- you heard me speak in
7 my opening comments about the need, a culture of doing things
8 as opposed to informing people about things. That's the
9 culture that exists within the bureaucracy and large parts of
10 the government, is that it's just about knowing things. And
11 when it comes to who's going to do something, those
12 conversations don't really happen there. And, at least,
13 that's been my experience.

14 **MR. CROFT MICHAELSON:** If I can just
15 interject, it's Croft Michaelson. You know, going forward,
16 there will be a lot of different players potentially
17 involved. There will be the Foreign Influence Transparency
18 Commissioner, CSIS, the RCMP, potentially the Commissioner of
19 Elections in certain types of scenarios.

20 And, you know, just to echo Mr. Paulson's
21 point, you know, when we've -- there needs to be -- there
22 will need to be some form of coordinating function, but at
23 the operational level, to sort out who's going to take the
24 lead on -- and what avenue is going to be pursued and what
25 makes sense.

26 You know, and in the national security -- in
27 the context of the counterterrorism space, I mean, the -- at
28 the operational level, the RCMP and CSIS sort of had those

1 type of mechanisms at the local level.

2 **DR. LEAH WEST:** So, currently, the SITE Task
3 Force exists, and it now exists throughout; it's not only
4 during the writ period. But do you see this overtaking the
5 SITE Task Force or being something that would be -- the SITE
6 Task Force would feed from it or complementary?

7 **MR. BOB PAULSON:** Well, I think building upon
8 that. I mean, the -- the seeming intent of the SITE Task
9 Force is to provide some mechanism for coordination of these
10 important issues, make sure that the police are in the room
11 and can -- but, to Croft's point, you know, there needs to be
12 that, okay, we understand, we understand what we know now,
13 what are we going to do about it, and what is the best way to
14 go about mitigating that or deterring it or stopping it? And
15 what are the consequences for everybody that's involved in
16 there?

17 I'm making it sound quite simple. It's a
18 very complex landscape. But absent the participation of all
19 the affected stakeholders, I don't think you can come to a
20 coordinated, you know, action.

21 And then, once things are underway, there's
22 nothing worse than having, you know, an ongoing criminal
23 investigation reported on into the government. Not because
24 of any other reason, other than those are very interesting
25 things to politicians, and they get out. So, it's not about,
26 you know, keeping our masters in the dark. It's about the
27 integrity of this investigative process that hopefully is
28 going to have an outcome. So, I think it would build on the

1 SITE Task Force. It would require the same sort of even more
2 elaborate governance that is provided for the SITE Task
3 Force.

4 **DR. LEAH WEST:** So, another element of
5 coordination -- we have about five minutes before the break,
6 three now, but I'll just -- we'll plant the seed -- is this
7 coordination amongst allies. And we are talking about
8 transnational activity that is affecting not just Canada, but
9 our allies, and we've seen that very recently in terms of the
10 charges against India or the allegations against India.

11 So, I'm just wondering if, Professor Currie
12 and Professor Wilner, if you had some quick remarks you
13 wanted to talk about, about how we leverage allies or how we
14 can improve upon the relationships with allies in this space.

15 **DR. ALEX WILNER:** I can be very quick.
16 Canada has yet to ever create a deterrence posture in any
17 domain. We function militarily within an allied setting.
18 And we're realizing quickly the limitations of acting in an
19 allied setting in cyberspace, where only at a certain
20 threshold, a very high threshold, where an allied response
21 might be expected. And so, we actually need our own cyber
22 deterrent posture. And I would suggest further, our own
23 specific posture related to foreign interference.

24 But those postures themselves would feed into
25 what we see internationally amongst allies, best practices,
26 and so forth. And so, it's a bit of a mesh, right? It's a
27 bit of an ecosystem of postures feeding into the end game of
28 deterring what we don't want to happen to us. Only then do

1 we prosecute and enforce. But deterrence is really the
2 bedrock, I would suggest.

3 **MR. BOB CURRIE:** Rob Currie, I'd only add, I
4 think, that I would get in line with the long line of
5 commentators who said it's time for new, rigorous, deep-
6 textured attention to foreign policy and formulating what it
7 looks like in the near term, in the medium term, in the long
8 term. In the way we've done in years past.

9 Again, that's a massive exercise, also, but
10 making sure that our foreign policy is geared to the current
11 threat environment. And I think that's, you know, that's
12 where we're living, the current threat environment. And the
13 perceptions of our allies along those lines, and specific
14 thought and attention to whether we are properly building
15 relationships, properly maintaining existing relationships,
16 whether it's NATO, whether it's Five Eyes, whether it's, you
17 know, any number of collective networks Canada is a part of.

18 With regard to what we're talking about on
19 this panel, we bring a very aware, border-porous kind of
20 posture around criminal law enforcement as part of the tool
21 bag to that table, as has been done in the past. There's
22 much to build on historically, both in our relationships and
23 the way we've administered them domestically. But a clear-
24 eyed and far-sighted attention to those relationships and how
25 they -- how they're going to support our own domestic
26 integrity as well.

27 **DR. LEAH WEST:** Commissioner, I think we'll
28 take a break?

1 **COMMISSIONER HOGUE:** Yes, we'll take the
2 break. Thirty (30) minutes. So we should be back at around
3 3:30.

4 --- Upon recessing at 3:00 p.m./

5 --- La séance est suspendue à 15 h 00

6 --- Upon resuming at 3:45 p.m./

7 --- La séance est reprise à 15 h 45

8 **COMMISSIONER HOGUE:** You can begin.

9 **DR. LEAH WEST:** Thank you.

10 So we received a lot of questions. Some of
11 them more specific, some of them more general. We're going
12 to start -- I'm going to ask Professor Currie to give us an
13 international law lesson.

14 In the last couple of days, we've heard a lot
15 about the diplomatic tools, and including PNGing diplomats
16 for example. There's been some questions about why we can't
17 prosecute or what would be required to prosecute a diplomat
18 who is engaged in foreign interference in Canada. I'm just
19 wondering if you could explain the legal barriers or
20 impediments in that regard?

21 **MR. ROB CURRIE:** Sure. This is Rob Currie.
22 This is -- rests on a network of law that helps states get
23 the day-to-day business done, because they have to interact,
24 governments have to have their personnel interacting, they
25 have to have people on the ground in foreign countries, and
26 for that work to get done, the work of diplomats and other
27 kinds of officials can't be interfered with by local law
28 enforcement.

1 Now, there are trade offs. And this
2 represents very much a trade off that countries make and
3 agree to. They say that, "We will send out diplomats to your
4 foreign capital, our ambassador or ambassadorial staff,
5 people who are accredited as diplomats, and you will accept
6 that, because of the importance of the job and the importance
7 of international discourse, that you won't allow your police,
8 your law enforcement mechanisms to interfere with them,"
9 meaning they are immune from the process of the courts, they
10 are immune from arrest, they are immune from the exercise of
11 jurisdiction locally.

12 Now, that's not to say that they're immune
13 and they can do anything. They are meant to actually follow
14 the local law, abide by it quite assiduously. Where this
15 becomes a harder-edged inquiry is when they don't. When a
16 person who enjoys that level of immunity commits a crime or
17 otherwise gets themselves in trouble in the foreign country.

18 The immunity keeps them from being
19 immediately arrested or otherwise detained or interfered with
20 by the state, but there is a diplomatic process on top of
21 that. So in a situation where a foreign accredited diplomat
22 commits a crime or is implicated in a crime, the host
23 government is not only empowered, but entitled under
24 international law to ask the sending government, "We want to
25 prosecute this individual. Please waive their immunity."

26 Now, that practice differs entirely based on
27 the nature of the crime, the countries involved. The U.S.
28 makes those requests fairly frequently. They are fairly

1 frequently granted. They are infrequent here in Canada,
2 though there is recent history with them.

3 The foreign states have the choice, and the
4 choice is waive the immunity, which means the individual can
5 be prosecuted, or refuse to waive the immunity, which means
6 they can't be, but then the final step of that process is
7 that the host government is free to, and usually does expel
8 that person. That's where the phrase *persona non grata* comes
9 from. They are ruled to be a person of no legal status.
10 They must immediately leave the country.

11 That's at the level of diplomacy. There's a
12 similar layer of protections with consular staff. It's more
13 limited. There are geographical limitations. There's a lot
14 of technical material there, but the basics are the same.

15 **COMMISSIONER HOGUE:** And can you just tell
16 me, do they sometimes waive the immunity? Or it's something
17 that is rarely seen?

18 **MR. ROB CURRIE:** In Canada, I can't think of
19 a case where the foreign state agreed to waive immunity.
20 Expulsion is normally how these things happen. I know in --
21 the only other country I'm aware of much of their practice is
22 the U.S., where they do manage to convince sending
23 governments to waive, very often in narcotics cases and
24 things like that. But in Canada, it's very, very unusual.

25 **DR. LEAH WEST:** Could you just speak to the
26 likelihood of it being waived in a case that involves foreign
27 interference?

28 **MR. ROB CURRIE:** If we do things the way

1 Professor Wilner has explained them, and we articulate these
2 demands, then in a way it won't create any worries, because
3 the state will be so ashamed of having engaged in foreign
4 interference that they will either immediately recall their
5 diplomats, or potentially allow for prosecution. But again,
6 the likelihood is not large. The states that are inclined to
7 interfere with us if their immune personnel are caught doing
8 it, they are most likely going to be recalled and immunity --
9 so they will continue to enjoy the immunity, but the
10 Government of Canada is fully empowered to push them out of
11 the country.

12 **DR. LEAH WEST:** Thank you. I want to return
13 to a discussion we had earlier, and as well this morning,
14 about this concept of laying charges as a signalling and as a
15 revelation of -- or at least a modicum of accountability for
16 people who aren't necessarily in Canada or who have left the
17 country after engaging in foreign interference.

18 And I just want to clarify the example of the
19 United States, and they're frequently doing this was raised
20 as an example, and I'm just wondering if, Mr. Michaelson, you
21 can speak to the differences and/or any similarities in how
22 that process occurs in the United States versus in Canada?

23 **MR. CROFT MICHAELSON:** Are you speaking to
24 the -- it's Croft Michaelson. You're speaking to ---

25 **DR. LEAH WEST:** Yes.

26 **MR. CROFT MICHAELSON:** --- the charging?

27 **DR. LEAH WEST:** The charging where you --
28 someone is outside of the country and -- versus the laying of

1 an indictment in the United States.

2 **MR. CROFT MICHAELSON:** Well, so in the United
3 States, they have a practice of, in their indictments, they
4 draft their indictments, they are really a narrative of the -
5 - and fairly extensive narratives of the conduct that
6 underlies and leads to the ultimate charge. So it's a
7 charging document, but it has a very, very long narrative.
8 And they can run into the tens, I've seen indictments that
9 are, you know, 50 or 60 pages long in the United States, and
10 those documents -- anyone reading that document will really
11 understand, to a large extent, the nature of the allegations
12 and the conduct that is being alleged against the individual
13 named in the indictment.

14 In Canada, charging documents are very
15 different. Whether it's an Information or an indictment,
16 those just specify the charge or charges that are alleged
17 against the accused. We don't go into large-scale narratives
18 of all the allegations. We prefer to argue our cases in
19 court and furnish the evidence in the context of the trial
20 proceeding.

21 So they're very different.

22 You know, investigations in the U.S. are also
23 quite different. They tend to be directed by a prosecutor.

24 So either -- at a superficial level, you have
25 everybody, sort of the District Attorney. You know, District
26 Attorneys they will often be involved in directing an
27 investigation. Same with at the federal level, Assistant US
28 Attorneys working together with the FBI, are very much

1 involved in the investigation.

2 In Canada, we have separate independent
3 functions. We have the investigative function, which is the
4 policing function, and we have the prosecution function,
5 which is an independent function. So there are those
6 differences as well as between Canada and the United States.

7 **DR. LEAH WEST:** But Mr. Paulson, forgive me
8 if I'm wrong, but I seem to recall in my past, large-scale
9 announcements where there's Mounties standing in front of
10 seized, I don't know, drugs or guns or whatever; you know,
11 these are prior to prosecution. So there is some element of
12 information or narrative that could accompany a charge, could
13 it not?

14 **MR. BOB PAULSON:** Oh sure, yeah. And I think
15 that, you know, we do that with, you know, varying degrees of
16 competency in terms of making those announcements. In the
17 case of Belmokhtar, where we charged, I think we -- you know,
18 first of all, we had to secure the Attorney General's consent
19 to bring that charge. They do an analysis of the public
20 interest in bringing that charge, and we were fairly vocal in
21 terms of announcing the charge.

22 I think everybody understood that it was
23 unlikely that we would get him back, but there's an
24 opportunity there to communicate the effort and the work, and
25 short of a conviction at least demonstrate the competency of
26 the criminal justice system to address those things.

27 More broadly, you know, now that I'm retired
28 several years I find myself yelling at my television as

1 police officers get up to make an announcement only to say,
2 "It's an ongoing investigation, it's before the courts, we
3 can't say anything." So you wonder why they're there in the
4 first place. I think there's opportunities to be a little
5 bit more strategic, in terms of giving information that will
6 not compromise the ongoing investigation or the prosecution,
7 with a view to sensitizing Canadians to what's going on.

8 **MR. CROFT MICHAELSON:** And if I can just
9 interject? It's Croft Michaelson.

10 I can tell you prosecutors hate press
11 releases by police because of the potential for compromising
12 a fair trial down the road. And so there -- to Mr. Paulson's
13 point, there's a balance. The police can say some things but
14 if they too far, then we have concerns about impacting on the
15 fair trial rights of the accused.

16 **DR. LEAH WEST:** Okay. So on the topic of
17 strategic disclosures -- there's a segue for you -- there's
18 strategic disclosure around charges, informing people of the
19 alleged offences, but also in the context of intelligence.
20 And I'm just wondering if you can speak to the deterrent
21 effect, or how that plays into deterrence, and if you could
22 provide some examples?

23 **DR. ALEX WILNER:** Sure. It's Alex Wilner
24 speaking.

25 In the leadup to the Ukraine -- I'm sorry; in
26 the leadup to the Russian invasion of Ukraine, there was a
27 very dramatic series of strategic public disclosures by high
28 officials in Washington, the UK, Canada to a degree, some of

1 these were disclosed -- some of these events took place out
2 of the White House, sometimes it was the State Department, if
3 I'm correct, sometimes they were within an Allied setting.
4 And the idea there was to illustrate to the Russians, and to
5 their leadership particularly, that their intent was known,
6 that their means were known, and that there was momentum to
7 counter it by a variety of means. And I think part of the
8 deterrent messaging around that was to get into Russian
9 leader's head; "Where are the leaks? How do they know this?
10 What kind of threats do I face? What are the costs that I
11 can't see at the moment?" And so it's to try to change and I
12 would say cloudy their perspectives of the use and utility of
13 that form of aggression in Ukraine.

14 It's possible that in -- you know, taking it
15 back to today's discussion, it's possible that in this world
16 of foreign interference, that you can imagine well-placed,
17 timely public disclosures by officials -- I won't say
18 military officials but officials, could perhaps get under the
19 skin of a foreign operator who's attempting to interfere in
20 Canadian elections or, more broadly, in other matters.

21 How that would work? I mean, I think it
22 needs to be studied. I think I would be curious -- as a
23 scholar would be curious to see if there's evidence in other
24 jurisdictions, but I think name and -- naming and shaming has
25 perhaps a public -- sorry; a deterrent effect. Doing so
26 within the Allied setting, once again, would establish kind
27 of a lockstep approach to countering interference. And it's
28 again, perhaps one more toolkit in the box, right, to kind of

1 nudge an adversary away from these types of engagements with
2 us.

3 **DR. LEAH WEST:** So I'm formulating this
4 question on the fly, so I apologize. But the -- I guess what
5 is the difference -- and maybe anyone can speak to this --
6 between strategic disclosures and warning? You know, because
7 in effect in the Russian example they were the same thing.
8 And one of the big concerns we hear so often in the
9 discussion around foreign interference in democratic
10 processes is that warning itself could affect the democratic
11 process, or it could diminish trust in democratic
12 institutions.

13 So is it different in this space? Should it
14 be different, or do you see it as having a similar effect?

15 **DR. ALEX WILNER:** Alex Wilner speaking.
16 I think the focus is here is not just
17 warning, right? It's the strategic disclosure of
18 intelligence, secret information. So handpicked information
19 that we will associate to an understanding of our adversary's
20 calculus. So it's not just a public warning, we think this
21 is happening. It's very tailored, I would say niche, and
22 it's meant to insert ourselves and our capabilities into an
23 adversary's calculus, and to sow confusion, disorientation,
24 and uncertainty in their ability to do what they want to do;
25 deny, deny their ability to do so, or to the costs that they
26 can't yet see. And I think that's the point. And you do it
27 in advance.

28 There's a concept of deterrence, there's

1 general deterrence; I'm powerful, you know it, don't mess
2 with me. And then there's very technical deterrence, at the
3 level of an event, we see you doing this, we think you're
4 doing this, we know how to respond, we're getting ready to do
5 so. And I think, you know, I'm not exactly sure where, which
6 type of deterrence we're talking about at the moment, but
7 it's not general deterrence; it's specific deterrence around
8 specific events, and I would imagine that goes beyond just
9 warning, it's more detailed and calculated.

10 **DR. LEAH WEST:** So that is potentially an
11 element of threat disruption, in a sense; you're identifying
12 the potential threat and saying, "we see you coming, and
13 we're prepared to stop it," to get people to change course.

14 There are other elements of threat disruption
15 or threat reduction, and we've heard through the evidence
16 about potentially law enforcement choosing not to pursue
17 criminal prosecutions, but rather choosing to disrupt or
18 reduce the threat through other means. And I'm wondering if,
19 Mr. Paulson, you can speak to how that might play out; if you
20 have any thoughts on the validity or the usefulness of threat
21 reduction activity by criminal law enforcement, and where --
22 and who might be best placed to engage in that kind of
23 activity?

24 **MR. BOB PAULSON:** Yeah, well, I would say
25 this; you know, the police have, as their primary function,
26 the investigation of crimes. But they also have a duty to
27 prevent crimes. And when investigating, if you come to an
28 assessment that there's unlikely, or having regard for

1 partner activity, better ways of going about it, then often
2 you can just confront.

3 You know, there's a term in surveillance
4 called overt surveillance. I'm not suggesting that's a good
5 technique, but it is one technique of allowing the target to
6 know he or she is under surveillance. And that changes their
7 approach to what they're doing. Often a confrontation of the
8 target or associates to the target can be useful at deterring
9 their activities. But that has to be very carefully weighed
10 against the likelihood of evidence collection or activities
11 of other partner agencies.

12 I'd also say this, getting back to
13 disclosure. There's a tactical advantage to sometimes having
14 these disclosures of evidence, or of intelligence, in terms
15 of, you know, the vernacular is kicking the anthill once
16 you're positioned to collect evidence. And that has a very
17 positive impact in terms of generating evidence, wiretap or
18 surveillance evidence, or witnesses, or sources, or
19 undercover operators that are close. So that is also a
20 useful tool.

21 **DR. LEAH WEST:** Can you speak a bit about
22 engagement at the -- sorry, I'm trying to formulate. It's
23 been a long day.

24 **MR. BOB PAULSON:** Local law enforcement?

25 **DR. LEAH WEST:** Yeah, crime prevention at the
26 local level.

27 **MR. BOB PAULSON:** So the *RCMP Act* requires
28 that the RCMP prevent crime. Most police agencies, municipal

1 police agencies, the two provincial police agencies that
2 exist, three, I guess, have as their duty to prevent crime.

3 And so I was going to observe earlier in our
4 discussions that there is a vast network and infrastructure
5 of avenues into communities, diasporas, and just ground-level
6 access to individuals in order to socialize, inform folks,
7 community policing officers. You know, the philosophy of
8 community policing is alive and well and applied in varying
9 degrees to even federal policing, in terms of engagement with
10 communities. And we rely -- one of the benefits to having
11 the RCMP engaged in contract policing is that access to local
12 information.

13 I'll point out that recent headlines relating
14 to India, you know, had a murder investigation being
15 conducted by a contract division giving rise to an
16 understanding of what was going on, and then coordinating
17 through federal policing and on to government to get the
18 outcome that we're seeing.

19 So that can't be undersold, that network of
20 police officer contact at local level, and the ability to
21 access that and to leverage that, in whatever the agenda'd
22 item is, is invaluable, frankly. And we've used that
23 extensively with -- in counterterrorism in the day. So it's
24 a powerful, powerful tool that sometimes gets overlooked.

25 **DR. LEAH WEST:** Professor Nesbitt, you've
26 written in the past on threat reduction, and I'm just
27 wondering your thoughts on threat reduction or disruption by
28 law enforcement and anything to consider in terms of that?

1 **DR. MICHAEL NESBITT:** Yeah, I guess my
2 addition would be to sort of reinforce a number of things
3 that Mr. Paulson has just said, and then just to offer a
4 slight warning.

5 And so to reinforce it, I mean, law
6 enforcement does all sorts of things to reduce threats;
7 right? So if there's an immediate threat, you're going to
8 take action to stop a bomb from going off, rather than say,
9 "Hold on, we're going to let it go off because we've got to
10 build a case." Right? Clearly that is going to happen.

11 Over the longer term, we do anything from
12 visiting schools to inform kids to community policing, which
13 can be really effective in terms of talking to communities
14 about what's going on and figuring out sort of things.

15 In the national security space, on the
16 terrorism side of things, we have all sorts of things across
17 the country where we do this sort of work. So where I'm from
18 in Alberta, we have the Organization for the Prevention of
19 Violence, the OPV, that does work with young individuals
20 usually, or historically, on counter-radicalization or
21 deradicalization in that space, right, as sort of an
22 alternative to charging.

23 So clearly lots of space for this work.

24 You do have to be careful. And I say that
25 primarily because we have CSIS for this very reason, which is
26 that in the 1970s, after the FLQ crisis and the invocation of
27 the *War Measures Act*, it was -- with the Macdonald Commission
28 then in 1984 and then the creation of CSIS, it was thought

1 that when you give a police agency intelligence powers with
2 disruption powers, that there might be incentive to use the
3 disruption powers, rather than the policing. It's easier. I
4 don't have to go do all the work to get a 300-page warrant
5 and spend a year gathering that evidence.

6 And so rather extreme example obviously, but
7 we did see a series of abuses over a number of years; right?
8 So from opening hundreds or thousands of pieces of mail to
9 burning down a barn in one case, where they thought an
10 individual had -- where individuals were meeting.

11 So I think the lesson from that just can't be
12 lost, which is that we've gone through it once where we said
13 the gold standard maybe isn't the prosecution, just as a
14 general sense, without guardrails, and we, in Canada, have
15 seen that once go off the rails as a result.

16 The final thing that I'll just say here, just
17 to add to what's been said is in 2015, CSIS was given
18 disruptive powers and that was reinforced and made what I
19 would argue to be more constitutional in sort of, I think it
20 came in 2019, but through 2017, Bill C-59 Act. And one of
21 the purposes of that was this very thing, was to say, "Look,
22 this is the intelligence agency. They sometimes need
23 disruption capacity, and so -- and we feel they require it."
24 And so it was CSIS then that was given the powers, but in
25 being given the powers, they were given guardrails, and those
26 guardrails were warranted. And I mean that in the legal
27 sense; they have to go get a warrant. And that just ensures
28 further disruptive activities under section 12.1 of the *CSIS*

1 Act.

2 DR. LEAH WEST: Speaking of Bills that got a
3 lot of attention, C-51 and C-59, they were subject to a lot
4 of debate, study, review, there was a lot of input at the
5 committee process by civil liberties groups on the most
6 recent, other than the last one, big national security Bill
7 C-70, because of the imperative, presumably, around having
8 things in place for future elections did not go through that
9 same level of scrutiny, and civil liberties groups decried
10 that because of the lack of study about potential *Charter*
11 impacts.

12 I'm wondering if any of you sitting around
13 this table have concerns about either the fact that there was
14 a lack of study of potential impacts and hearing of those
15 voices in the Bill moving forward, or any specific provisions
16 or elements of the Bill that you think are particularly
17 problematic?

18 And I'll start with Professor Nesbitt,
19 because -- because.

20 DR. MICHAEL NESBITT: So we're talking about
21 a bill that's very new. So I say that because while having
22 read the Bill, I have not had time to formulate my thoughts
23 on the details.

24 Now, I suppose that goes to the point, which
25 is that there aren't very many of us in this space and sort
26 of *post hoc* we're trying to figure out our view on the Bill.

27 I will add, you know, the other question
28 there is not just the *Charter* compliance, although that's

1 obviously always a good question. The other is whether
2 there's something missing, right, that maybe more could have
3 been done through consultations. And I refer back to my
4 earlier conversation about sort of taking a broader approach
5 to thinking about the mandate and structure of the
6 organization and how it engages with other organizations. So
7 I don't know, but at some point it would be nice to have that
8 opportunity, I suppose, for Canada.

9 **DR. LEAH WEST:** Mr. Michaelson, do you have
10 any thoughts.

11 **MR. CROFT MICHAELSON:** Well, the Department
12 of Justice, on their website, they have their *Charter*
13 statement, as they're required to do, and, you know, they've
14 indicated that in their view, the legislation is
15 constitutional, the Attorney General is required to turn
16 their mind to the legislation and whether it's
17 constitutional.

18 And I frankly think that they take those
19 functions very, very -- those responsibilities very
20 seriously, so I think that they are primarily of the view
21 that the legislation is constitutional.

22 You know, nothing leapt out at me as I was
23 looking at it, but again, as Professor Nesbitt said, it's
24 early days and one never knows, you know, what arguments a
25 smart and creative defence lawyer can come up in a reasonable
26 hypothetical argument at trial.

27 You know, we've had other legislation that's
28 gone forward and no doubt everybody thought it was

1 constitutional, and it was found to be unconstitutional
2 because of reasonable hypotheticals that no one had thought
3 about.

4 So again, it's early days and we'll see.

5 **DR. LEAH WEST:** Thank you. Now I want to
6 turn back to potentially some of the provisions that have
7 been added to the *Criminal Code*.

8 But Professor Currie, if you could expand on
9 your discussion of seizing opportunities to use
10 extraterritorial jurisdiction in the foreign interference
11 space?

12 **MR. ROB CURRIE:** Sure. Rob Currie. And let
13 me bounce off the last one as well, because here is an aspect
14 of C-70 that won't be a problem under the *Charter*, which is
15 the expansion of the territorial reach of some of the
16 offences.

17 And I say that because there have been legal
18 challenges to extraterritorial criminal law provisions in the
19 past under a theory that it was somehow offensive to
20 individual rights, and that is -- it's incorrect -- it's an
21 incorrect argument and because it's a matter of
22 constitutional power and federal government is fully
23 competent to legislate in a manner that makes -- extends our
24 criminal law beyond our shores if they choose to do so.
25 There are limits, but they are limits imposed by
26 international law, not by domestic constitutional law.

27 So I think that's -- you know, that's just a
28 point worth making. Extending the geographical reach of law

1 enforcement doesn't impinge on *Charter* rights by itself.

2 But to get into the weeds of what that means,
3 I think the best way to explain it is to take a hypothetical
4 FI case, which is one person who is, you know, an agent of a
5 bad actor state making threats, intimidating remarks maybe,
6 or bribes, or that kind of activity.

7 There are three levels, jurisdictionally, at
8 which it might be done.

9 It might be done entirely on Canadian soil,
10 and we don't have a problem. That crime happened entirely in
11 Canada, Canada is fully jurisdictionally competent.

12 But what if the bad actor is telephoning the
13 individual from another country or sending them email --
14 threatening email threatening their family? Does Canada have
15 jurisdiction to do anything? Can the police even look at
16 that?

17 And again, anecdotally, that can be a
18 problem. Somebody walks into a police station and says, "I'm
19 getting these threatening emails. I think I know where
20 they're coming from." And the poor under-resourced cop says,
21 "They're coming from outside of Canada. We can't do anything
22 about that." And legally, that's not true, but resource-
23 wise, to an extent, it is true.

24 But that's an example of what's referred to
25 technically as qualified territorial or extended territorial
26 jurisdiction. If a crime begins outside Canada but finishes
27 here, we have jurisdiction over it. If it begins here and
28 finishes outside Canada, we have jurisdiction over it. And

1 there's an extensive body of case law around that.

2 But in C-70, there are also fully
3 extraterritorial provisions, which is to say the entire
4 offence takes place outside Canada. And those are situations
5 where Canada can completely lawfully, under international
6 law, take jurisdiction over the offence, even though it's
7 entirely outside our borders, based on some other link to our
8 national interests, to our nationals, sometimes. And the
9 examples we see in C-70 are situations where either the
10 perpetrator, or the victim, or both are Canadian nationals,
11 they're outside Canada, which is -- which extends it right
12 out, or that other Canadian national interests are
13 implicated, because there's a slightly murky but still well-
14 worn principle of international law that says states can
15 criminally prosecute crimes that take place outside their
16 borders if they are -- if those crimes are directed at their
17 fundamental national interests. And this is everything from
18 espionage to counterfeiting of passports and currency.

19 But foreign interference activities, I would
20 offer, fall right in neatly into that pocket of things Canada
21 is absolutely competent to do.

22 So all three of those levels of jurisdiction
23 are available to Canada. The ones that touch outside our
24 borders are the ones that historically we've been
25 uncomfortable with. And I say historically because it comes
26 from the U.K., where for centuries they didn't care what
27 happened off the island. It didn't matter what happened in
28 France. It matters more than ever now what happens outside

1 Canada that potentially impacts us.

2 So there is a really good set of
3 jurisdictional tools, and C-70 really is beginning to crack
4 that open, and I just say we should break it even further
5 open.

6 **DR. LEAH WEST:** One of the parties asked a
7 question about a tool that is fully extraterritorial in
8 scope, which is the *Crimes Against Humanity and War Crimes*
9 *Act*. Do you see that as a potential tool in the context of
10 foreign interference?

11 **MR. ROB CURRIE:** I think the short answer is
12 no. And you're right, that's -- that part of our criminal
13 law provides a set of offences that do apply entirely
14 extraterritorially, as well as within Canada, but it is on
15 the subject of a really narrow range of crimes, literally
16 three: genocide; crimes against humanity; and war crimes.
17 And I think we can expect that those three kinds of conduct
18 won't play a large role, if any, in foreign interference
19 efforts.

20 **DR. LEAH WEST:** Commissioner?

21 **COMMISSIONER HOGUE:** I'm okay. You can go
22 on.

23 **DR. LEAH WEST:** I'm just going to invite the
24 panellists to offer any last remarks that they might have or
25 that they want to convey to the Commission, or things that
26 they want to, you know, double stamp on.

27 Professor Wilner?

28 **DR. ALEX WILNER:** Thank you. Alex Wilner

1 speaking.

2 I want you to imagine a world where
3 deterrence doesn't work. It's not pretty; right? It means
4 that we're responding repeatedly with no understanding of the
5 larger things that we could do. And so deterrence is, again,
6 -- my takeaway is deterrence is something you actively do.
7 You think about it, and you apply it, and you tie all of
8 those loose strings that we have going now, and you tie it to
9 this core, which is don't mess with us. Don't mess with us.
10 We have the means to deny the success. We have the means to
11 prosecute. We have the means to attack you if needed.

12 Until we link all of these pieces together,
13 it's the early days of counterterrorism, whack-a-mole. One
14 there, one there, one there, one there. We keep responding.

15 So deterrence again is just simply a
16 framework that feeds into this entire soup of activity. And
17 I think it ties neatly into what we can do domestically and
18 internationally because we're not doing it alone.

19 So I think we need a bit of a shift.

20 And finally, one last piece is that from a
21 deterrence scholarship, we're still stuck in the Cold War
22 logic of deterrence, which was success or failure. If the
23 nuclear bomb goes off, deterrence failed. But we're not --
24 that's not the kind of deterrence we're into. We're kind of
25 leaning into criminal deterrence, which is we put up with a
26 certain threshold of pain, but to a certain degree beyond
27 that, we bring the hammer down.

28 And so I think when we speak of deterrence,

1 we should take it out of the Cold War context, we need to
2 internationalize it, and update it, and expand it, but it
3 needs to be within the context of what we're facing today,
4 which is a mess, which is an absolute mess. But I think it
5 is the bedrock upon which all of the other pillars can rest.

6 **DR. LEAH WEST:** Could you just briefly speak
7 to how you see denial working in terms of building trust in
8 democratic institutions, public education? How does that
9 feed into your framework?

10 **DR. ALEX WILNER:** The logic of denial is to
11 strip an adversary the ability to acquire what it hopes to
12 acquire with the unwanted act.

13 And so denial here in this case is to, I hate
14 to use this word, but to inoculate Canadian society against
15 responding in the ways that our adversaries would like for us
16 to respond when they engage with disinformation, which is to
17 ultimately change my vote, or to undermine the credibility of
18 legal system, or our democratic system, et cetera.

19 And so we saw this again going back to the
20 early days of counter-radicalization, the idea was to
21 inoculate people, societies, communities, against falling
22 into this trap, radicalization in one case. In this case,
23 acting upon disinformation or foreign interference.

24 And so I think denial is sending the message
25 that we are able to absorb and ignore the things that you
26 send our way. This is not exclusively or even solely about
27 what the Federal Government can do. I think public education
28 is part of this. I think it's about engaging with scholars

1 and setting up communities of practice, and all the rest;
2 right? But I think denial is part and parcel, because we can
3 only punish so much, but denial is about how we protect
4 ourselves and link that to manipulating behaviour.

5 **DR. LEAH WEST:** Thank you. Anyone else? Mr.
6 Paulson.

7 **MR. BOB PAULSON:** I think we need to consider
8 why it is that we are being victimized the way we are
9 recently. And what weakness that demonstrates or is being
10 exploited by those hostile state actors. I think it's
11 absolutely vital that we get our act together, because it's a
12 harbinger of what's going to come. Weakness breeds an
13 invitation to do more.

14 And I think the perception, and this is very
15 anecdotal, but I think the international perception,
16 particularly among our adversaries, is that we are vulnerable
17 to exploitation. And so, that should just maybe underscore
18 the importance of your work.

19 **MR. CROFT MICHAELSON:** If I could just make
20 an interjection briefly. It's Croft Michaelson. There's
21 been some discussion about strategies such as laying charges
22 against individuals outside of the country where there may be
23 little prospect of prosecution actually going forward.

24 And I think the practical reality is that for
25 police that are under-resourced, that's not going to be a
26 strategy that they're going to be interested in pursuing.
27 And prosecutors probably won't be particularly interested in
28 it either. It really calls for, if this is a priority, it

1 really calls for proper resourcing of both the police and
2 investigative function -- the police and prosecutorial
3 functions.

4 You know, if I think back, you know, and Bob
5 will remember this too, but when you think back to the early
6 days of the *Proceeds of Crime* legislation, when that first
7 came out in the 1980s, we didn't really get -- make a lot of
8 headway initially, and then we set up specialized units. And
9 the specialized units then had, you know, identified it as a
10 priority activity, and then we started to make a lot of
11 headway in investigations and successful prosecutions.

12 So, no doubt the Commissioner's heard about
13 resourcing in other -- in other roundtables, but I think
14 that, you know, it's central to actually having an effective
15 prosecution function.

16 **DR. LEAH WEST:** And this will turn into an
17 excellent segue to my question for Professor Nesbitt, which
18 is you spoke a bit about money and sanctions. I'm just
19 wondering about your thoughts as sanctions and their
20 deterrent effect in this space, and if you could speak to
21 that.

22 **DR. MICHAEL NESBITT:** I think -- so if I may
23 give you the technical answer, I think the academic
24 literature over time is largely split on the actual
25 deterrence effect of sanctions. Having said that, the more
26 recent work I have seen would seem to suggest that sanctions
27 do have a deterrent effect. I also have serious questions
28 about whether we're measuring the right thing in a number of

1 those studies.

2 So, just anecdotally speaking, when we
3 sanction Russia, very quickly there's a Russian response to
4 sanction a bunch of high-profile Canadians. So, what does
5 that tell you? They're paying attention, they care, and they
6 feel like they need to respond. So, I guess that gets me to
7 my feeling about this, which is that it is hard to study this
8 space or just watch this space and not think that sanctions
9 have a meaningful deterrent effect.

10 Having said that, we have to be honest about
11 where Canada sits in the sanctions space, and that is as an
12 economically smaller player, beside and supportive of the
13 United States, and I suppose the last thing I'll say in that
14 regard is that when we're talking about sanctions, there's
15 only so much we will do. A lot of it is for supporting the
16 U.S., and if the U.S. is doing something, then sanctions will
17 have a deterrent effect.

18 But I will say our lack of -- it's perhaps,
19 once again, an opportunity to bring up our lack of
20 enforcement, right? So in 1992, we have the *Special Economic*
21 *Measures Act*, and we have two prosecutions to date under the
22 *Special Economic Measures Act*. One of which fell apart at
23 pre-trial, and the other, which was a guilty plea for what
24 was literally sending stuff to Iran in contravention of our
25 Iran regulations, and the border catches it and says, "You
26 can't send this stuff to Iran." So, pretty easy capture.

27 And so, in the absence of that enforcement,
28 which we have been working, and there has been good headway

1 in the last four or five years at Foreign Affairs with
2 funding for the RCMP, and then RCMP setting up sort of
3 sanction resourcing within the broader sort of national
4 security and money areas, we're getting there, but we haven't
5 seen those results yet. And until we start seeing those
6 results, Canada's ability to deter or contribute to the
7 broader deterrence goals of our allies, particularly the EU,
8 the U.K., Australia, and the U. S. on the sanctions side, is
9 pretty limited.

10 **DR. LEAH WEST:** And my last question is for
11 Professor Currie, before I turn it over to the Commissioner.

12 Are there any other international fora
13 besides international courts where you could see Canada
14 taking its concerns over FI that might be useful, or other
15 convention bodies, et cetera, or do you really see pursuing
16 international legal measures at say the ICJ as the only tool
17 internationally?

18 **MR. BOB CURRIE:** The ICJ, it's not even a
19 great tool. You know, those proceedings are time-consuming,
20 they're contentious and expensive, and you always run the
21 risk that the foreign state on the other side will withdraw
22 their agreement to consent to the Court's jurisdiction. So -
23 - and it's been stunning in cases where they didn't, in fact.
24 So, there are layers of politics there.

25 But this is more on the informal end of
26 enforcement. It's more about relationships with allies,
27 presenting united fronts and really appearing to have a
28 robust domestic framework that is outward-looking and that

1 will counter the authoritarian and meddling forces that are
2 coming at us. That's no less enforcement of international
3 rights and obligations than going to court is. It's just a
4 different and, frankly, more historically grounded way of
5 doing it.

6 **DR. LEAH WEST:** Thank you.

7 Commissioner?

8 **COMMISSIONER HOGUE:** I have one question for,
9 I think it will be for Mr. Michaelson. You have a lot of
10 experience in prosecuting various crimes. And I'm interested
11 in knowing whether you have any ideas as to how to minimize
12 the impact of the intelligence-to-evidence problem. In the
13 context of if, for any reason, the decision will be made to
14 prosecute foreign interference, can you think of any means of
15 minimizing this problem?

16 **MR. CROFT MICHAELSON:** Well, the best way to
17 minimize the problem is to rely on as little intelligence
18 information as possible, obviously.

19 I do think there may be room for some
20 statutory reform of the section 38 disclosure regime. I
21 think that, you know, my prosecution in the *Regina v. Jaser*
22 case, you know, we navigated the national security issues in
23 that case, I thought, quite successfully. I thought that
24 what Justice Code came up with in *Regina v. Jaser*, you know,
25 might be a useful template on how to, you know, how one could
26 actually reform the section 38 disclosure regime and invest
27 jurisdiction in a Superior Court trial judge to address the
28 issues.

1 You know, absent that, you know, now, we have
2 -- the disclosure regime we have has been one that's been
3 crafted, you know, by the Supreme Court of Canada. They've
4 always said there may be more than one disclosure regime
5 that's constitutional. And so, whether one looks at some
6 outside-of-the-box thinking and really thinks about, you
7 know, having an alternative approach from the one we're
8 thinking about, something like intelligence information, I've
9 thought about this a lot and I really haven't cracked the nut
10 yet, Commissioner, so there's not much more I can add on.

11 **COMMISSIONER HOGUE:** It's not an easy one.

12 **MR. CROFT MICHAELSON:** Yeah, it's not an easy
13 one. I had some ideas in a paper that I wrote that was
14 published in the *Manitoba Law Journal*, you know. Some of it
15 was blue-sky thinking, and I'm not sure that it would
16 actually ultimately make things much better. But I don't
17 really have any easy answer for you.

18 **COMMISSIONER HOGUE:** Thank you.

19 So thank you very much. It was interesting,
20 challenging, and what is fascinating is you have many
21 different experience; many different field where you have an
22 expertise, so I will have to put all that all together and
23 try to find our way in that context.

24 But I really, really appreciate all the
25 information you have provided me with today. And again, I
26 have said that on a few occasion, but it's really food for
27 thought for us, and we realize how much work we have ahead of
28 us.

1 So thank you, and have a good day, all.

2 **MR. CROFT MICHAELSON:** Thank you.

3 --- Upon adjourning at 4:34 p.m./

4 --- L'audience est ajournée 16 h 34

5
6 **C E R T I F I C A T I O N**

7
8 I, Sandrine Marineau-Lupien, a certified court reporter,
9 hereby certify the foregoing pages to be an accurate
10 transcription of my notes/records to the best of my skill and
11 ability, and I so swear.

12
13 Je, Sandrine Marineau-Lupien, une sténographe officielle,
14 certifie que les pages ci-hautes sont une transcription
15 conforme de mes notes/enregistrements au meilleur de mes
16 capacités, et je le jure.

17 
18 _____

19 Sandrine Marineau-Lupien
20
21
22
23
24
25
26
27
28